Information Fusion 127 (2026) 103718

Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

Towards scalable indoor positioning systems (IPS): User-centric challenges, methods, and recommendations for user-friendly crowd-powered framework

Ahmed Mansour [a,b,*], Wu Chen [a], Eslam Ali [c,b], Jingxian Wang [a], Duojie Weng [d]

[a] Department of Land Surveying and Geo-Informatics, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
[b] Department of Public Works, Faculty of Engineering, Cairo University, Giza, Egypt
[c] Department of Building and Real Estate, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
[d] Ministry of Natural Resources (MNR) Key Laboratory for Geo-Environmental Monitoring of Great Bay Area & Guangdong Key Laboratory of Urban Informatics, Shenzhen University, Nanshan, Shenzhen, China

ARTICLE INFO

Keywords:
Crowdsourcing
Indoor positioning systems
Scalability
Privacy and security
Incentive mechanisms
Data quality
Mobile crowdsensing

ABSTRACT

Crowd-powered Indoor Positioning Systems (IPS) offer a cost-efficient and scalable alternative to traditional site-survey-based methods for generating the offline prerequisites of ubiquitous, measurement-driven IPS. However, the widespread adoption of such paradigms depends on resolving critical user-centric challenges that span all layers of the crowd-powered architecture. This survey provides a systematic investigation of these challenges, including user participation schemes, incentive mechanisms, privacy and security threats, and the impact of data collection and localization on user devices. To the best of our knowledge, this is the first in-depth review that examines these issues and their implications for data quality, reliability, and scalability, with a specific emphasis on user-friendliness. It maps these challenges across the architectural layers of crowd-powered IPS, reviews prior studies to analyze the user's role and assigned tasks in active, opportunistic, and passive participation schemes, emphasizing the objectives of these tasks and the trade-offs associated with each scheme. Next, it distinguishes incentive mechanisms in crowd-powered IPS from those in other domains, highlighting how intrinsic and extrinsic motivations can be aligned with IPS-specific objectives. It then surveys the mathematical models employed in current incentive mechanisms, along with their goals and limitations. Subsequently, it reviews the privacy and security risks, the preservation techniques proposed in existing literature, and their shortcomings. In addition, the survey discusses the adverse impacts of data collection and localization on user devices, identifying potential user burdens and associated mitigation strategies. Finally, it outlines a roadmap of recommendations for developing user-friendly, sustainable, and scalable IPS.

1. Introduction

With the growing complexity of urban infrastructures, indoor positioning systems (IPS) have become vital for navigation in unfamiliar buildings where Global Navigation Satellite Systems (GNSS) fail due to signal blockage or attenuation. The proliferation of IoT devices and smartphones intensifies demand for enhanced indoor Location-Based Services (LBS) [1] across different applications and sectors. This ever-rising demand underscores the urgent need for scalable IPS that can be globally deployed using readily available buildings and mobile device resources [2,3]. Scaling IPS is also necessary to handle the growth of the indoor positioning market, which is projected to expand from USD 20.38 billion in 2023 to values ranging between USD 95 billion and USD 146.09 billion by 2030, with compound annual growth rates (CAGR) estimated at 37.6 % [4] and 42.63 % [5,6], respectively.

1.1. Barriers to scalability in IPS

While this period may be regarded as the "*golden age*" of IPS [7], marked by breakthroughs in indoor ranging technologies, achieving scalability remains a formidable challenge. Existing IPS often rely on external hardware, including deploying sensors or devices in buildings or smartphones, both of which incur significant costs and hinder scalability [8]. Other systems require the pre-construction of offline prerequisites. For instance, trilateration and triangulation-based systems depend on precise knowledge of reference locations and propagation

* Corresponding author.
E-mail addresses: ahmed.m.mostafa@connect.polyu.hk (A. Mansour), wu.chen@polyu.edu.hk (W. Chen).

https://doi.org/10.1016/j.inffus.2025.103718
Received 11 February 2025; Received in revised form 18 August 2025; Accepted 2 September 2025
Available online 17 September 2025
1566-2535/© 2025 Elsevier B.V. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

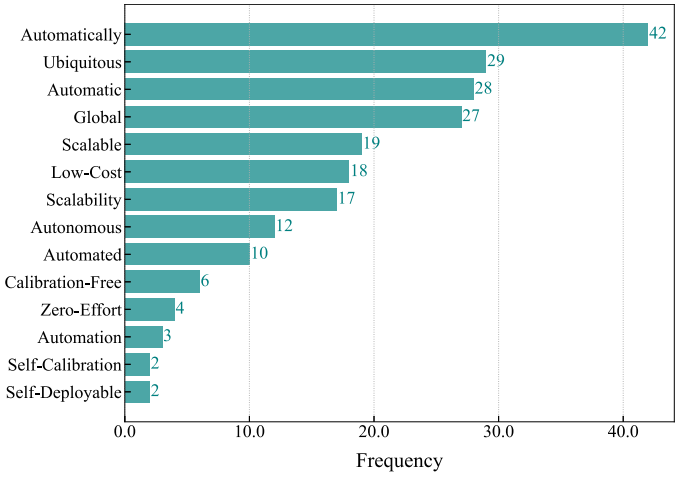

Fig. 1. Frequency of automation- and scalability-related terms across titles, abstracts, and keywords in the surveyed literature on crowd-powered indoor positioning.

parameters [9]. In contrast, range-free systems, including those based on magnetic fields or Wi-Fi received signal strength (RSS) fingerprinting, show promise for scalability due to the ubiquity of their measurements. However, these systems face significant hurdles, including a reliance on labor-intensive offline site-survey mapping and difficulty adapting to dynamic environments [10]. Automating the generation of these offline prerequisites is critical to achieving scalable IPS.

1.2. Crowd power role in breaking IPS scalability barriers

A paradigm shift in IPS emerged with the revolutionary idea of empowering users or crowds to act as autonomous surveyors. By seamlessly integrating the data generated during their daily activities, this approach enabled the creation of large-scale, offline IPS prerequisites without requiring dedicated survey efforts. Faced with the impracticality of manually creating and frequently updating radio and magnetic fingerprint maps across indoor environments on a global scale, IPS has emerged as a proving ground for crowd-powered solutions that seek to balance accuracy and reliability with operational feasibility. Since their initial application to IPS in 2012, such approaches have increasingly prioritized automation and scalability. This shift is consistently reflected in the literature, where recurrent terms such as ***calibration-free, automatic, self-calibration, zero-effort, low-cost, global, scalable, ubiquitous, self-deployable,*** and ***autonomous*** dominate titles, abstracts, and keywords. As shown in Fig. 1, these terms underscore the research community's sustained focus on developing efficient, low-effort, and scalable IPS solutions.

1.3. Developmental milestones and emerging trends in crowd-powered systems

Crowd-powered systems can be historically traced to the foundational concept of *crowd wisdom*, introduced by Surowiecki in 2004 [11], which posits that collective intelligence can, under the right conditions, surpass the decision-making capabilities of individuals [12]. The historical trajectory of these crowd-powered paradigms is illustrated in Fig. 2. Over the past two decades, technological advancements and the proliferation of mobile devices have driven the evolution of this concept, leading to the emergence of *crowdsourcing*, a paradigm popularized by Howe in 2006 [13]. Crowdsourcing enabled the outsourcing of tasks to large groups, leveraging their collective skills and resources. Building on these foundations, *participatory sensing* emerged as a key innovation, empowering individuals to gather and share local data using personal devices like mobile phones [14]. With the advent of smartphones equipped with advanced sensors, this concept further evolved into *smartphone sensing*, which enabled more efficient and scalable data collection [15]. The culmination of these advancements led to *mobile crowdsensing (MCS)*, a paradigm that leverages the ubiquity of mobile devices to facilitate data collection on an unprecedented scale [16]. This evolution has been fueled by the exponential growth of connected devices, projected to exceed 18 billion globally by 2025 [17], surpassing the global human population. MCS exploits the ubiquity and sensor richness of smartphones to enable large-scale, decentralized, and cost-effective data collection. Such connectivity has fostered diverse MCS-driven innovations [18], spanning urban planning, environmental monitoring, healthcare systems, smart city infrastructure, transportation optimization, and disaster management, with continual expansion into novel domains. Since its formal introduction, and particularly over the past decade, MCS has evolved into a well-established and mature research paradigm that has witnessed significant growth, marked by substantial empirical and theoretical advancements and evidenced by a broad range of retrospective surveys and application-oriented studies. MCS has been increasingly adopted in a variety of *domain-specific applications*, demonstrating its versatility and societal relevance. By way of example, not limitation, Cicek and Kantarci [19] highlight the role of MCS in disaster response systems, Zhang et al. [20] explore its integration in healthcare monitoring, and Xiao et al. [21] investigate its application within vehicular networks for intelligent transportation solutions. In addition, these advancements are well documented in a range of *retrospective surveys and landscape reviews*. Examples of such contributions include, but are not limited to, Capponi et al. [18], presenting an in-depth synthesis of architectural designs, system components, and operational challenges that characterize the MCS ecosystem; Liu et al. [22], adopting a data-oriented perspective that structures MCS systems around the data life cycle while highlighting challenges in quality, transmission, and processing; Suhag and Jha [23], offering an updated review of MCS frameworks and applications with emphasis on context-awareness and service integration; and Dasari et al. [24], examining game-theoretic models for user participation and incentive mechanisms. Collectively, these works provide a multidimensional perspective on the evolution of MCS, encompassing system design, data management, and user-centric strategies. In parallel, the literature on the *topical evolution of MCS* has deepened our understanding of critical design aspects such as privacy, security, and user incentives. Notable contributions in this area include Gisdakis et al. [25], who reviews security and trust frameworks; Zhao et al. [26], who address sparse data scenarios and inference challenges; and Wang et al. [27], who propose privacy-preserving task management models. Together, these studies underscore the trajectory of MCS from a conceptual innovation to a foundational component in contemporary ubiquitous sensing ecosystems.

While we explored the historical evolution of crowd-powered paradigms, it is important to clarify the common yet often ambiguous usage of the terms *crowdsourcing* and *crowdsensing*. Although closely related, these terms are not synonymous, and the distinction is particularly critical in the context of IPS. **Crowdsourcing** typically refers to leveraging contributions from a large group of individuals, often involving *explicit user input, manual annotation, or task-based problem-solving*. By contrast, **crowdsensing** (or mobile crowdsensing) refers to the collection of sensor data from users' mobile or wearable devices. This may occur either *opportunistically*-such as through the background collection of Wi-Fi signals-or *participatorily*, when users are prompted to perform specific sensing tasks (e.g., scanning QR codes, walking predefined paths, or capturing measurements). It is worth briefly noting at this stage that, within the IPS domain, data acquisition relies more on *crowdsensing* than on *crowdsourcing*, due to its emphasis on passively collected, device-generated sensor data instead of explicit human annotation. A more detailed differentiation between these terms, including the degree of user intervention and the role of participants in crowd-powered IPS, is provided in Section 3, where user involvement is classified into *active* (closely aligned with the notion of crowdsourcing) and

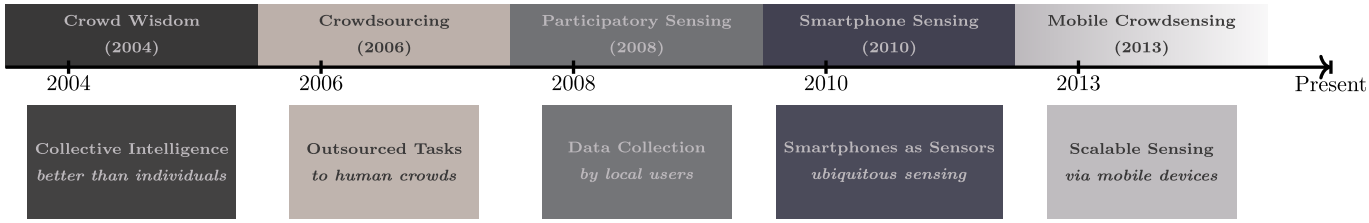

Fig. 2. The historical evolution of crowd-powered paradigms.

opportunistic or *passive* (more representative of crowdsensing). To maintain clarity throughout this survey, we adopt the term ***crowd-powered IPS*** as an umbrella concept that encompasses both crowdsourcing- and crowdsensing-based approaches. This term is used in contexts where both paradigms are applicable or intertwined.

1.4. User-centric challenges and research gaps

Undoubtedly, the success of crowd-powered approaches, including MCS and crowdsourcing, relies heavily on user contributions, whether through passive or active participation. The dual role of users as both sources of data and consumers of the service amplifies the importance of ensuring acceptance to engage and satisfaction [17]. This success is contingent upon effectively addressing user-centric challenges and ensuring a user-friendly system design [28]. Key user-centric challenges include minimizing the burden and distraction for participants by optimizing the balance between active and passive intervention, motivating and incentivizing users, ensuring privacy and security, and mitigating the impact of user contributions on device performance. While crowd-powered paradigms have been widely adopted across various domains, their application in IPS presents significantly greater user-centric challenges than in other fields [29], ultimately constraining system scalability. This amplification arises due to the stringent requirements for fine-grained spatial data, the continuous need for data collection in dynamic environments, and heightened privacy concerns associated with indoor localization data.

Despite the growing application of crowd-powered paradigms in IPS, with over 238 publications to date and approximately 20 research works published per year (refer to Fig. 3), a thorough investigation of the literature reveals a notable gap, which is a lack of comprehensive reviews addressing these user-centric challenges in IPS. A deep investigation of existing reviews on crowd-powered IPS, as referenced in Table 1, reveals that they have predominantly focused on technical aspects, such as underlying technologies [30], layered framework for data integration [31], and low cost annotation methods [32], while largely neglecting studies that address user-centric issues, including user-friendly participation, incentive mechanisms, privacy preservation, and the impact on device performance. However, these challenges form the cornerstone of the practical applicability of crowd-powered paradigms in IPS. Pei et al. [30] emphasized the use of crowd-sensed opportunistic signals for indoor localization, reviewing cost-effective approaches for generating and updating fingerprint databases. While their work highlighted signal diversity, it primarily addressed technical concerns such as device heterogeneity and signal variability rather than user-centric aspects. Similarly, Zhou et al. [31] introduced a layered framework for reviewing crowd-powered indoor localization, providing a structured overview of technologies and methodologies without a dedicated focus on user challenges. Wang et al. [32] discussed fingerprint crowdsourcing challenges, including device diversity and environmental variability. However, none of these surveys systematically addressed user-centric challenges in IPS, except for Lashkari et al. [29], which classified crowd-powered indoor localization approaches based on user participation levels and site-survey dependencies without explicitly tackling the broader user-centric concerns of crowd-powered IPS.

Other surveys have reviewed user-centric challenges in crowd-powered paradigms in general without being restricted to a specific field of application within MCS, such as privacy [22], incentives [33], and data quality [34], as summarized in Table 2. However, these challenges are further amplified in IPS due to the unique constraints and requirements of indoor localization [29,35]. For instance, privacy concerns were reviewed by Liu et al. [22] for MCS applications, but in IPS, even if the data is totally anonymized, these concerns are even more critical due to the sensitivity of fine-grained indoor location data. In domains such as traffic management and vehicular networks [36,37], the collected data may partially approach buildings where users reside but do not capture the fine-grained details of their daily lives and routines behind walls. Unlike other domains, where data may be more generalized, crowd data for IPS directly reflects user behaviors, movement patterns, and preferences. This level of detail increases the risk of security breaches, as exposed data could reveal sensitive personal information [38]. Consequently, addressing privacy and security in IPS is more critical than in other domains to safeguard users and encourage participation. Similarly, while incentive mechanisms for MCS applications have been reviewed independently in [33]. Compared to other fields, IPS-specific requirements place greater demands on user incentive mechanisms to ensure sustained user participation and maintain data reliability. Addressing the adequacy of existing incentive models for IPS remains an open research question, necessitating deeper investigations. Data quality, another critical challenge, was generally reviewed by Restuccia et al. [34] in the context of MCS. In fact, coarse-grained data may suffice for domains such as environmental monitoring or disaster response. In contrast, data quality in IPS presents greater challenges due to the necessity for fine-grained data to ensure reliable radio and magnetic fingerprinting and accurate indoor LBS. In domains where coarse-grained localization data is sufficient, factors such as sensor bias, device heterogeneity, and environmental interference may have a negligible impact and often do not require user feedback. However, in IPS, user contributions and feedback play a more critical role in mitigating these uncertainties, making user engagement more valuable compared to other domains. This creates a significant trade-off between user-friendliness and reliability in IPS, which is more pronounced compared to other domains. Another crucial challenge is energy consumption, which has been reviewed in the context of MCS by Wang et al. [39]. However, energy efficiency becomes a more severe issue in IPS due to the dense and intensive sensing requirements necessary for precise localization. Unlike other MCS applications, IPS demands more data collection and high-frequency updates, leading to greater strain on mobile device resources and battery life, making energy consumption a critical concern in IPS compared to other MCS applications, as it impacts both system sustainability and user willingness to participate.

Overall, while MCS and crowd-powered paradigms have demonstrated promise across various domains, their application in IPS presents unique and amplified user-centric challenges. Therefore, there is a pressing need to address the unique user-centric challenges and domain-specific requirements associated with implementing crowd-powered paradigms in IPS. Tackling these challenges is essential to enhancing the scalability, practicality, and widespread adoption of MCS-driven IPS solutions.

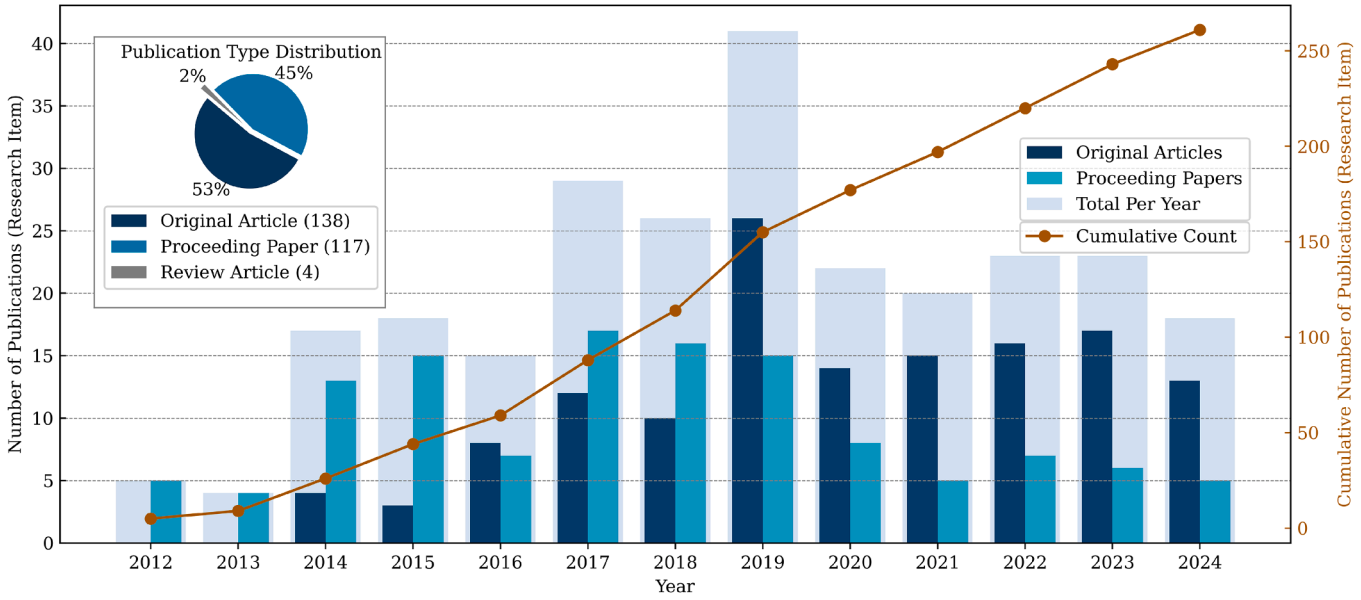

Fig. 3. Publication trend in crowd-powered IPS. The left vertical axis represents the number of publications per year, depicted as stacked bar plots categorizing original articles, proceeding papers, and total articles per year.

Table 1
Comparison of related surveys on crowd-powered IPS.

Study	Year	4*Main Focus	User-Centric Challenges			
			User Role	Incentives	Privacy	Impact on Device
[30]	2016	Crowd-sensed opportunistic signals for cost-effective fingerprint database generation	✗	✗	✗	✗
[32]	2016	Challenges of fingerprint crowdsourcing, including device diversity	✗	✗	✗	✗
[31]	2018	Layered framework for system architecture and signal integration	✗	✗	✗	✗
[29]	2018	Classification of user roles into crowdsourcing vs. crowdsensing approaches	✓	✗	✗	✗
This Survey	2025	User-centric challenges and the impact on scalability and reliability.	✓	✓	✓	✓

Table 2
Existing reviews on user-centric challenges in mobile crowdsensing (MCS) and the heightened impact of these challenges in the field of MCS-driven indoor localization.

Survey	Challenge	Key Points	Heightened Impact in Crowd-Powered IPS
[22]	Privacy	General privacy concerns in MCS, where anonymization is typically sufficient for data protection.	Fine-grained IPS data reveals detailed indoor movement patterns, raising heightened privacy risks. Even anonymized data can expose behavioral details, necessitating stricter privacy-preserving mechanisms tailored for IPS.
[33]	Incentives	MCS research reviews general incentive mechanisms for user participation.	Unlike outdoor crowdsourcing, where data is often collected in streets and open spaces, inherent dynamic indoor environments present additional complexities as they consist of different types of buildings and floor diversity, with comprehensive spatial coverage; refer to Section 4.4.1 for detailed comparison. Current models may not sustain long-term engagement, creating an open research challenge.
[34]	Data Quality	Some MCS applications (e.g., environmental monitoring) can tolerate coarse-grained data, with quality issues having a limited impact.	IPS requires fine-grained, high-quality data for accurate positioning. Sensor bias, device heterogeneity, and environmental interference significantly affect reliability, making user feedback more critical than in other domains.
[39]	Energy Consumption	Energy efficiency is a consideration in MCS, where sensing is periodic and less resource-intensive.	IPS requires more data collection than other fields and frequent updates, creating significant energy consumption challenges. This necessitates energy-efficient localization strategies beyond those explored in general MCS research.

1.5. Systematic search, multi-stage screening process, and dimensional categorization

To bridge this gap, a comprehensive literature search was conducted across three major academic databases, Web of Science (WoS), Scopus, and IEEE Xplore, to identify studies on IPS within crowd-powered paradigms. As illustrated in Fig. 4, the search targeted publications whose titles, abstracts, or keywords explicitly contained *"indoor positioning," "indoor localization," or "indoor navigation"* in combination with *"crowd*," "crowdsourced," "crowdsensing," or "crowd-powered"*. Equivalent queries were adapted to each database's syntax, as presented in Fig. 4, with the WoS example being:

TS = (("indoor positioning" **OR** "indoor localization" **OR** "indoor navigation") **AND** ("crowd*" OR "crowdsourced data" **OR** "crowdsensing" **OR** "crowdsourcing"))
AND LANGUAGE: (English) **AND**
DOCUMENT TYPES: (Article **OR** Proceedings Paper **OR** Review) **AND PUBLICATION YEARS:** (2012–2024)

.

The TS field searches titles, abstracts,and keywords simultaneously. The search was restricted to peer-reviewed English-language journal articles, conference papers, and review papers, while editorials, short papers, and unrelated crowd-powered applications were excluded. The initial search identified 1561 records (403 from WoS, 608 from Scopus,

and 542 from IEEE Xplore), which, after duplicate removal, yielded 485 unique items. A first screening of titles and abstracts excluded 205 off-topic items, followed by the removal of 101 duplicate studies representing conference and journal versions of the same work, resulting in 179 items for full-text review. Of these, 153 focused on other IPS challenges rather than directly addressing user-centric aspects; this subset included 41 studies that generated a radio map from scratch or updated it using crowd data (reviewed to identify user roles and impact), and 107 studies excluded for concentrating on unrelated topics such as fingerprint localization algorithms or purely technical calibration. To ensure comprehensive coverage, 88 additional relevant publications were incorporated from outside the initial search results, focusing on user-centric challenges in general MCS applications and strategic recommendations relevant to IPS. The final review encompassed 148 publications, classified into four user-centric dimensions:

- User Intervention: 41 studies, where those proposing radio map generation from scratch or updating using crowd data were examined to determine the type of user intervention required. The classification distinguished between active user participation, in which users perform specific actions, and passive data collection, in which crowd data is gathered without direct user involvement.
- Incentives: 42 studies, of which six specifically introduced incentive mechanisms for crowd-powered IPS, while the remaining studies targeted incentives in other domains or in general MCS applications.
- Privacy and Security: 38 studies, including seven focused on privacy in MCS-based IPS, whereas the remainder addressed privacy within broader MCS contexts.
- Impact on Devices: 4 studies, with one examining the impact of data collection on devices in IPS, while the other three investigated this aspect in the context of general data collection and mobile positioning applications.

The selected studies were systematically analyzed to identify prevailing user-centric challenges, evaluate methodological approaches, and review case study evidence.

1.6. Key questions and contribution points

A deep investigation of existing related studies reveals several critical unanswered questions. Addressing these questions is essential for effectively tackling user-centric challenges in future research, ultimately contributing to the scalability of IPS. Among these key questions are:

1. *User involvement-related questions*: What types of user intervention are employed in existing crowd-powered IPS studies? What kinds of tasks are assigned to users, and what are the objectives behind these tasks when active user intervention is involved? Specifically, are these tasks designed to ensure data quality and reliability? How do these tasks impact user willingness to participate, and are they practical and acceptable to a wide range of users without compromising scalability? What are the advantages and limitations of active and passive schemes? What are the dilemmas and trade-offs associated with choosing between active and opportunistic user involvement in crowd-powered IPS? If active involvement proves unavoidable, what are the recommended hybrid frameworks and key considerations for mitigating the limitations of both active and passive schemes and balancing data quality with user-friendly engagement while achieving scalability?
2. *Incentive mechanisms-related questions*: How do incentive mechanisms in IPS differ from those in other MCS-driven domains? What are the primary goals of IPS that incentives aim to support? What are the limitations and gaps in current incentive mechanisms for crowd-powered IPS? How can intrinsic and extrinsic motivations be combined to better aligned IPS goals? What other recommendations can enhance the design and implementation of incentive mechanisms in this domain?
3. *Privacy and security-related questions*: What are the primary privacy and security risks associated with MCS in IPS? How do existing studies address these risks? What limitations exist in current privacy and security mechanisms for crowd-powered IPS? What recommendations can guide the development of robust privacy and security mechanisms?
4. *Questions related to the impact of Data collection and localization on user device*: What are the potential adverse effects of crowd data collection and localization processes on users' devices? What limitations exist in current studies? What are the recommended strategies to mitigate the resource burden of data collection and localization on users' devices?

This survey aims to bridge the identified gap by providing a comprehensive review of user-centric challenges in crowd-powered IPS, including user engagement types, incentive mechanisms, privacy and security concerns, and the impact on smartphones. Additionally, this survey seeks to answer the key questions mentioned above to serve as a roadmap for guiding future research toward the development of user-friendly, crowd-powered IPS schemes capable of maintaining scalability. Specifically, the contribution points can be summarized as follows:

Firstly, we present a concise overview of the architecture and hierarchical layers commonly adopted in crowd-powered paradigms, with a specific emphasis on their application in IPS, as illustrated in the upper part of Fig. 5. To the best of our knowledge, this is the first work to provide a comprehensive discussion that maps user-centric challenges and issues to the corresponding architectural layers. It identifies the specific points where these challenges emerge and examines their impacts on key system metrics.

Secondly, we provide an in-depth survey on active, opportunistic, and passive user participation in existing crowd-powered IPS. To more comprehensively address the key questions surrounding user intervention type in crowd-powered IPS, we systematically discussed the distinct advantages, limitations, and user-engagement implications of both active and passive participation. Moreover, we conducted a quantitative assessment to evaluate the impact of different user involvement tasks and types on indoor positioning performance. This detailed analysis illuminates critical trade-offs and dilemmas for achieving scalability, ultimately guiding our recommendations for hybrid frameworks that effectively balance data quality, reliability, user-friendly engagement, and system growth.

Thirdly, we review user motives and the corresponding incentive mechanisms, including their potential integration and categorization, as presented in general MCS applications from the perspectives of user psychology and system design. This foundation enables a subsequent review of utility functions, pricing models, enabling technologies, and methodological approaches used for implementing and optimizing incentives and rewards, with particular emphasis on the interplay among these elements and the general implementation steps in real-world applications. Building on insights from general MCS applications, we then shift focus to provide an in-depth survey of existing incentive strategies and their underlying mathematical models within the context of crowd-powered IPS. In an effort to provide a robust answer to key questions related to incentive design challenges in crowd-powered IPS, we investigate the unique goals, constraints, and challenges inherent to these systems. This helps to shed light on the limitations of existing approaches and illustrates how combining both intrinsic and extrinsic rewards can help align IPS objectives. Additionally, we offer a quantitative assessment of the impact of the existing incentive mechanisms. Ultimately, these insights form the basis of our recommendations for crafting low-cost, practical, and robust incentive schemes that foster sustained user engagement and scalability.

Fourthly, we provide an overview of privacy and security risks and protection strategies across the MCS lifecycle. In addition, we review the key protection techniques for general MCS applications. Then, to address pressing questions and concerns around privacy and security in

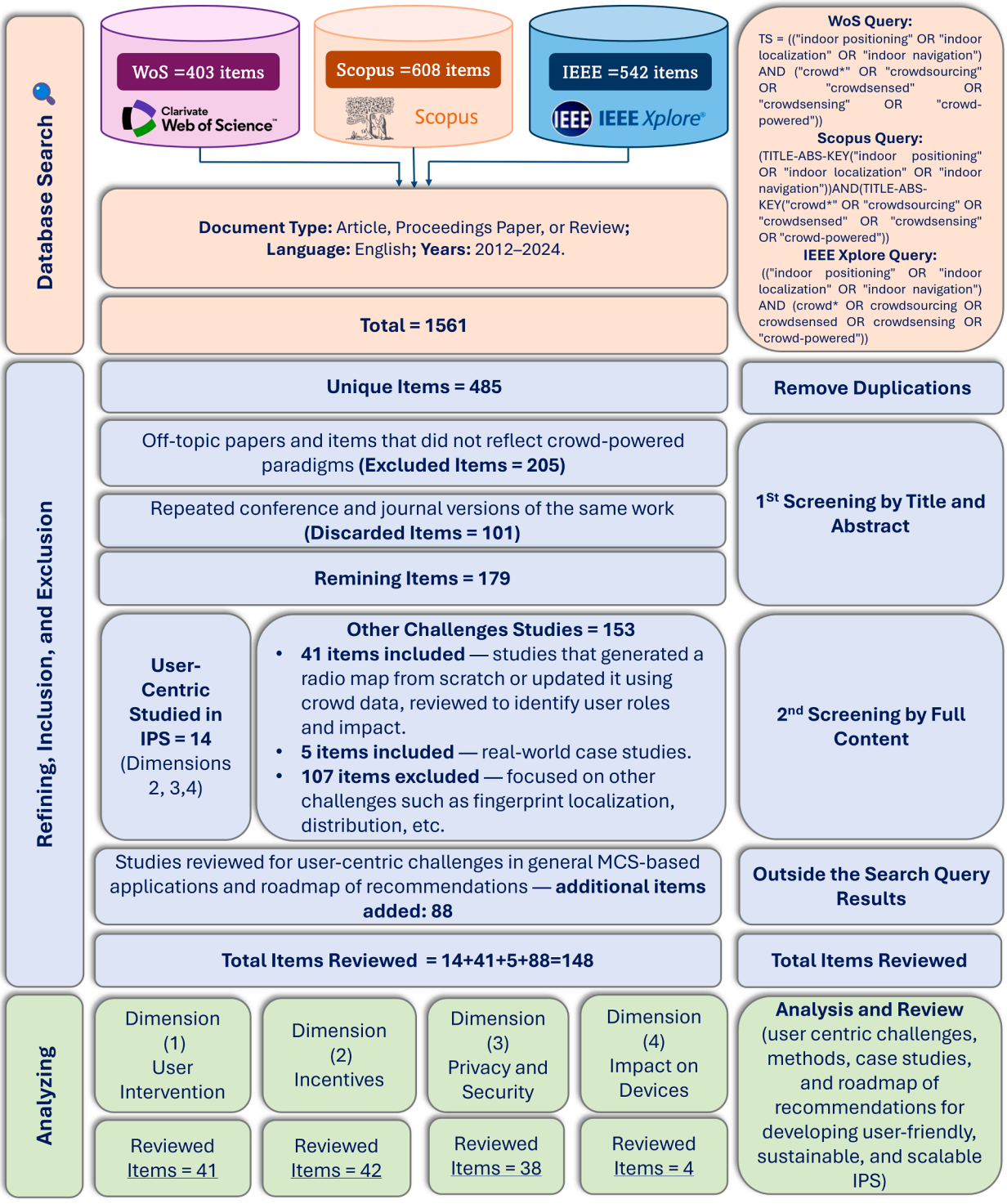

Fig. 4. Overview of the systematic review process used to identify and analyze user-centric challenges in crowd-powered IPS.

crowd-powered IPS, we systematically discuss prevalent vulnerabilities and review state-of-the-art techniques to protect sensitive data and their methods. This analysis reveals critical shortcomings of current frameworks, illustrating how advanced safeguards can preserve user trust while maintaining the integrity of large-scale IPS deployments. Ultimately, these findings guide our recommendations for developing robust, user-centric privacy and security schemes that ensure both data protection and scalability.

Lastly, we systematically analyze the adverse effects of extensive data collection and localization on user devices, spotlighting battery life, processing overhead, and overall experience. Our examination reveals critical gaps in current practices and demonstrates how strategic optimizations can preserve IPS accuracy without compromising usability. We conclude our review by evaluating notable large-scale real-world implementation case studies. Drawing on insights from both existing literature and practical deployments, we provide a set of practical

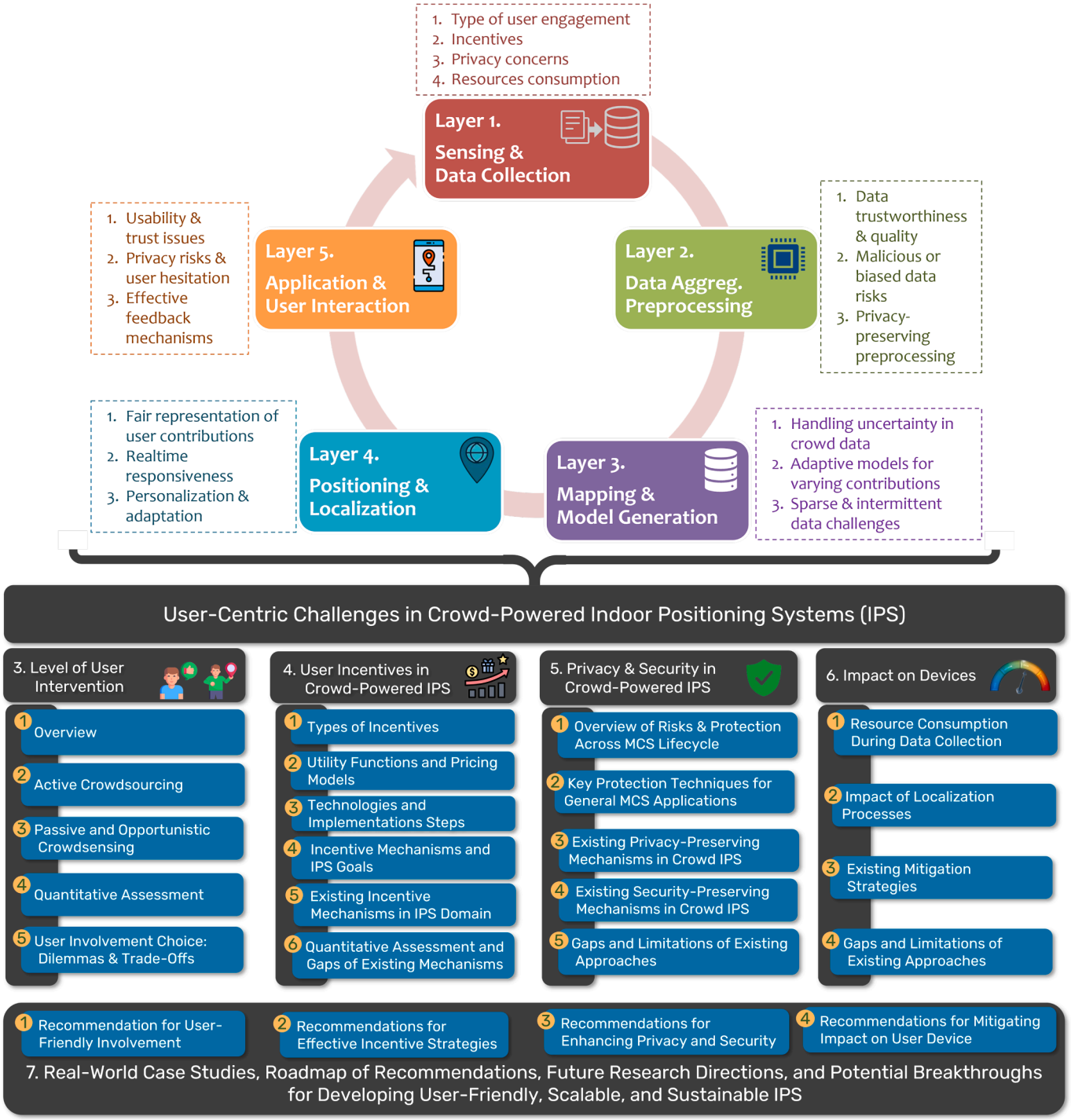

Fig. 5. Overview of the architecture of crowd-powered paradigms in IPS and the taxonomy of this survey paper. The upper part of the figure illustrates the architecture of crowd-powered paradigms in IPS, emphasizing user-centric challenges across hierarchical layers. The lower part of the figure outlines the structure of this survey paper.

recommendations, a unified theoretical implementation framework, future research directions, and potential breakthroughs aimed at developing lightweight, user-centric solutions that effectively balance performance and scalability.

The remainder of this paper is organized as follows: an overview of the structure is provided in Fig. 5. Section 2 provides a concise overview of the architecture and hierarchical layers commonly adopted in crowd-powered paradigms, specifically focusing on their application in IPS; refer to the upper part of Fig. 5. Section 3 reviews the levels of user intervention and their implications for IPS. Section 4 explores motivation and incentive mechanisms to enhance user participation. Section 5 discusses privacy and security challenges in detail. Section 6 analyzes the impact of data collection on smartphone performance and proposes strategies for mitigation. Finally, Section 7 concludes with real-world deployment case studies, recommendations for future research directions, and insights into building scalable, user-centric IPS. The abbreviations and their corresponding meanings used throughout this paper are summarized in Table 3.

Table 3
List of abbreviations.

Abbreviation	Meaning
ACTD	**A**bnormal **C**rowd **T**raffic **D**etection
AHP	**A**nalytic **H**ierarchy **P**rocess
AI	**A**rtificial **I**ntelligence
AnonCreds	**Anon**ymous **Cred**entials
AP	**A**ccess **P**oint
BERT	**B**idirectional **E**ncoder **R**epresentations from **T**ransformers
BLE	**B**luetooth **L**ow **E**nergy
CAGR	**C**ompound **A**nnual **G**rowth **R**ate
CP	**C**rowdsourcing **P**latform
CrowdBLPS	**Crowd**sensing **B**lockchain-based **L**ocation **P**rivacy **S**cheme
CrowdFL	**Crowd**sensing **F**ederated **L**earning
CSI	**C**hannel **S**tate **I**nformation
DP	**D**ifferential **P**rivacy
DPE	**D**ifferential **P**rivacy-**E**nabled
EI	**E**quilibrium-Driven **I**ncentive
ERC	**E**dinburgh **R**esearch **C**entre
FL	**F**ederated **L**earning
FLoc	**F**ederated **L**earning for **I**ndoor **Loc**alization
GNSS	**G**lobal **N**avigation **S**atellite **S**ystems
HE	**H**omomorphic **E**ncryption
IMU	**I**nertial **M**easurement **U**nit
IPS	**I**ndoor **P**ositioning **S**ystems
IoT	**I**nternet of **T**hings
KPI	**K**ey **P**erformance **I**ndicator
LBS	**L**ocation-**B**ased **S**ervices
LDP	**L**ocal **D**ifferential **P**rivacy
MCS	**M**obile **C**rowd**S**ensing
MFHE	**M**ulti-**F**unctional **H**omomorphic **E**ncryption
ML	**M**achine **L**earning
MU	**M**obile **U**ser
NFC	**N**ear **F**ield **C**ommunication
OPFL	**O**ptimized **P**ersonalized **F**ederated **L**earning
PARS	**P**rivacy-**A**ware **R**eward **S**cheme
PDR	**P**edestrian **D**ead **R**eckoning
PSM	**P**seudonym **S**coring **M**echanism
PST	**P**attern **S**imilarity **T**ree
POI	**P**oint **O**f **I**nterest
QDA	**Q**uality-**D**riven **A**uction
RBR	**R**esponders' **B**ehaviors-Based **R**eputation
RDF-SCF	**R**eputation-**D**riven **F**og-Assisted **S**ecure **C**rowdsourcing **F**ramework
RFID	**R**adio-**F**requency **I**dentification
RL	**R**einforcement **L**earning
RSS	**R**eceived **S**ignal **S**trength
RSSI	**R**eceived **S**ignal **S**trength **I**ndicator
SC	**S**ervice **C**ustomer
SCE	**S**patial **C**overage **E**xpansion
SMPC	**S**ecure **M**ulti-**P**arty **C**omputation
TEE	**T**rusted **E**xecution **E**nvironment
Wi-Fi	**Wi**reless **Fi**delity
ZKP	**Z**ero-**K**nowledge **P**roof

2. User-centric challenges across the architectural layers of crowd-powered IPS

This section offers a concise overview of the architecture and hierarchical layers commonly adopted in crowd-powered paradigms, with a specific focus on their application in IPS. Unlike prior reviews that often overlook architectural structures and their user-related implications, our discussion explicitly emphasizes the layered transformation of crowd-contributed data into actionable positioning insights. We also systematically map user-centric challenges to their corresponding architectural layers, identifying where these issues arise and how they affect system performance, reliability, and user adoption. This layered mapping enables a clearer understanding of the complex interplay between user participation and system efficacy, establishing a foundation for deeper investigation in the subsequent sections.

The architecture of crowd-powered IPS typically consists of multiple interdependent layers, each designed to perform specific roles in the data lifecycle, from acquisition to localization output. These layers collaboratively transform raw sensor data from user devices into reliable positioning outputs, as illustrated in Fig. 5. However, user-centric challenges, stemming from factors such as data trustworthiness, engagement variability, privacy concerns, and incentive limitations, emerge at different layers and can compromise the integrity of the entire pipeline. The general architectural layers and their associated user-centric challenges are outlined as follows:

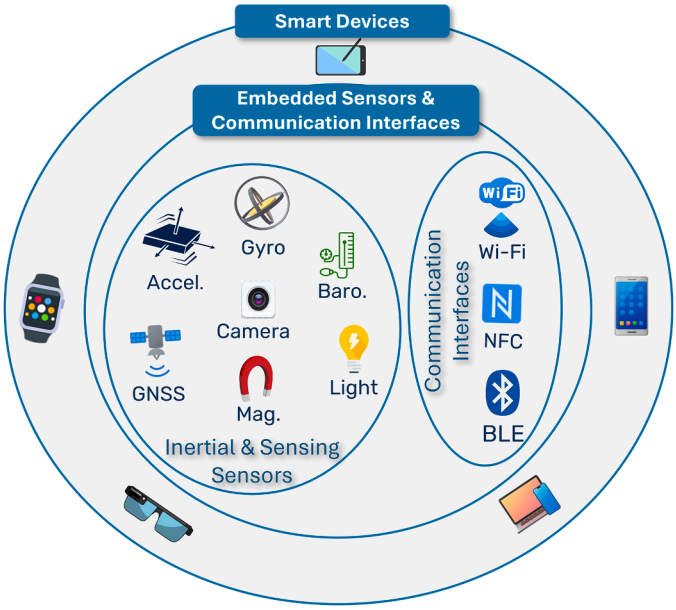

Fig. 6. Illustration of the sensing layer in crowd-powered IPS, showcasing smart devices equipped with embedded sensors (e.g., accelerometer, gyroscope, magnetometer, light sensor, barometer) and communication interfaces (e.g., Wi-Fi, BLE, and NFC).

2.1. Sensing and data collection layer

The sensing and data collection layer constitutes the backbone of any crowd-powered IPS system. It leverages the sensing capabilities of user devices, such as smartphones and wearables, to gather raw environmental and motion data. Embedded sensors, including accelerometers, gyroscopes, magnetometers, barometers, cameras, and light sensors, along with communication technologies such as Wi-Fi, BLE, and GNSS, contribute significantly to building a rich dataset. Fig. 6 illustrates the sensing capabilities of modern smart devices. These resources enable key functionalities such as indoor-outdoor detection, building-street clustering, floor identification, and 2D localization of collected radio and magnetic fingerprints. Additionally, they provide spatial references essential for global localization. A critical user-centric challenge at this layer is ensuring user engagement and participation, which will be discussed in Section 3. Crowdsensing systems heavily depend on voluntary, semi-voluntary, or incentivized contributions (as elaborated in Section 4). Users may be reluctant to share data due to privacy concerns (discussed in Section 5), energy consumption (covered in Section 6), or a perceived lack of personal or contextual benefit.

2.2. Data aggregation and preprocessing layer

Once collected, the data is transmitted to a centralized or distributed server for aggregation and preprocessing. This layer plays a critical role in transforming raw crowdsourced data into a structured, reliable format by filtering noise, handling missing or incomplete data, and ensuring temporal and spatial synchronization. These preprocessing steps are essential for making the data usable in subsequent modeling and analysis [40]. User-centric challenges at this layer primarily revolve around data trustworthiness and quality assurance, which are heavily influenced by

the type of user intervention and the mechanisms employed by the system to ensure high-quality contributions. Systems often rely on strategies such as offering monetary incentives or providing tangible value to users in exchange for their participation (as elaborated in Section 4). However, since crowdsourced data originates from diverse and independent users, there is an inherent risk of malicious or low-quality contributions, intentional falsification, or bias in reporting. These issues can compromise the reliability of the dataset and, consequently, the overall performance of the system. Another major challenge is achieving data reliability without introducing excessive computational overhead, which is crucial for scalability and real-time processing. Furthermore, the implementation of privacy-preserving mechanisms during preprocessing remains a significant concern (as discussed in Section 5). Balancing the need for effective data cleaning and organization with the imperative to safeguard user privacy is essential for maintaining trust and encouraging sustained participation. Robust techniques must be employed to address these challenges and ensure the integrity and usability of the aggregated data.

2.3. Processing and model generation layer

This layer is responsible for transforming processed data into meaningful spatial representations, providing various outputs that build the offline requirements of IPS and enable context awareness. One possible output is the *radio map*, which represents the spatial distribution of RSS signatures from existing Wi-Fi access points (APs) [41]. Also, the *location and propagation parameters* of these APs can be derived to facilitate multilateration-based positioning algorithms, improving accuracy in signal-based localization. Another possible output is the *magnetic map*, which captures spatial variations in the Earth's magnetic field induced by structural elements within buildings. It leverages *magnetic anomalies*, caused by steel reinforcements and other infrastructure, as stable reference points to enhance positioning robustness. Additionally, *floor-level BSSID distinction* can be generated by identifying unique Basic Service Set Identifiers (BSSIDs) associated with different floors, thereby enabling reliable multi-floor positioning. To further refine vertical positioning, *barometric pressure data* can be integrated, facilitating precise floor-level detection. Another possible output is a *building signature*, which is generated by integrating radio, magnetic, and environmental parameters, providing a unique identifier for each structure and ensuring seamless transitions between different buildings while maintaining localization continuity [42]. Furthermore, key spatial references, such as *landmarks [43] and points of interest (POIs)*, including escalators, entrances, and prominent Wi-Fi hotspots, can be inferred and embedded within the generated models to aid in navigation and map refinement. To support LBS, *shop and context-aware information* can be incorporated, enriching the map with metadata such as store names, facility types, and contextual attributes. This enhances the user experience and enables intelligent indoor services, including personalized navigation and contextual recommendations. By integrating these diverse mapping elements, this layer generates essential outputs that significantly improve the accuracy, reliability, and usability of indoor positioning systems.

A major user-related challenge at this layer is mainly the impact of user contribution on the data's uncertainty, quantity, and availability. User-generated data is often noisy, incomplete, or biased due to variations in device capabilities, sensor accuracy, and individual usage behaviors. Designing robust models that can adapt to these inconsistencies is essential for maintaining reliability. Additionally, user participation is typically sporadic and inconsistent, necessitating algorithms that can effectively handle sparse and intermittent data contributions. The overall efficiency, spatial resolution, availability, and scalability of the resulting models are closely tied to the quality and density of user-contributed data. This layer also plays a proactive role by identifying under-sampled regions, detecting gaps in fingerprint coverage, and signaling the need for improved data reliability in specific areas. Furthermore, it can support decision-making related to incentive design by analyzing data availability and quality, enabling the system to assign appropriate incentive types and distribution strategies. This ensures that data collection efforts are optimally directed toward enhancing coverage and accuracy where they are most needed.

2.4. Output layer: Positioning and localization layer

The decision-making or output layer takes the generated models, such as radio and magnetic maps, POI, and floor information, and then translates them into actionable outcomes. In the context of IPS, this may involve determining precise locations, updating indoor radio maps, or providing navigational instructions. This layer interacts with higher-level systems or applications, ensuring that the insights derived from the data are applied effectively. From a user-centric perspective, one of the key challenges is ensuring equitable representation and adaptive personalization. Since different users may contribute at varying rates and with different levels of accuracy, there is a risk that certain contributions may be undervalued or overlooked. Moreover, the system must be capable of responding to user feedback and behavioral patterns in real time, thereby adapting its outputs to improve usability and trust.

2.5. Application and user interaction layer

The user interaction and application layer is the topmost layer of the architecture. It provides interfaces for end-users or external systems to access and utilize the results generated by the system. This layer focuses on usability, This layer focuses on usability, presentation of results, and seamless integration into broader applications. In the context of IPS, it translates positioning data into user-facing services that support applications such as indoor navigation, asset tracking, and LBS in commercial or industrial environments. Its primary function is to ensure that end users can intuitively access and interact with the system, thereby realizing the practical value of the insights generated. User-centric challenges in this layer revolve around interface usability, user trust, and privacy protection. Users may hesitate to adopt or interact with crowd-powered applications if the interface is unintuitive, the information is perceived as unreliable, or privacy risks are not well addressed. Additionally, there is a need for effective feedback mechanisms to allow users to report errors, correct inaccuracies, and refine the system over time.

2.6. Concluding remarks

The layered architecture outlined above provides a structured lens through which to examine the interplay between technical processes and user-centric factors in crowd-powered IPS. By mapping specific challenges-ranging from engagement, trust, and privacy to data reliability and scalability-to their corresponding architectural layers, we establish a clear framework for understanding how user participation shapes system performance at every stage. This perspective not only highlights the interdependencies between layers but also sets the groundwork for the following section, which focuses on the varying levels of user intervention and their influence on the overall efficiency, reliability, and sustainability of crowd-powered IPS. In the following sections, we delve deeper into the user-centric challenges that arise across the architectural layers of crowd-powered IPS.

3. Level of user intervention

In this section, we investigate studies on crowd-powered IPS to identify the type of user intervention required in each case (i.e., whether it involves *active user involvement* or *opportunistic user involvement*). For studies involving active participation, we analyze the user's role and the specific tasks they were asked to perform. This enables an assessment of user abstraction levels, system usability, and overall user-friendliness. Additionally, we examine the rationale for requiring user participation, whether to ensure data quality, enhance reliability,

or fulfill other system-level objectives. Through this analysis, we offer a structured overview of the user-assigned tasks, their intended purposes, and their implications for user acceptance in practical deployments. The following sections present a detailed discussion of these findings, highlighting the advantages and limitations associated with each type of user involvement.

3.1. Overview of types of intervention

Crowd-powered IPS can be classified into three main approaches based on the level of user involvement: active, passive, and opportunistic. Active crowdsourcing relies on users explicitly participating in data collection. This means they *intentionally* contribute information, such as recording signal strengths or tagging locations. Passive crowdsourcing, in contrast, requires little to no effort from users. Data is gathered seamlessly in the background while they go about their daily routines, often without even realizing it. Opportunistic sensing removes user involvement entirely. Here, devices autonomously decide when and what to sense, leveraging data that naturally emerges as a byproduct of other activities. The fundamental difference between these approaches is the degree of user engagement. Active crowdsourcing requires deliberate user actions, passive methods operate unobtrusively in the background, and opportunistic sensing relies entirely on autonomous device behavior.

Table 4 presents a comparative analysis of user tasks, organized by the type of user interaction involved. For each task, it summarizes the associated user effort, expected data accuracy, reliance on user expertise, and scalability potential, supported by representative studies. The following subsection provides a detailed examination of these tasks as reported in existing crowd-powered IPS research.

3.2. Crowdsourcing: Active user intervention

3.2.1. Tasks assigned to users in active user intervention-based studies

In active user involvement approaches, individuals are directly engaged in the data collection and processing phases. Active user intervention has been suggested in several tasks, such as:

1. Asking User Feedback: User feedback plays a crucial role in enhancing the accuracy and reliability of crowd-powered IPS. In certain studies, participants are actively involved in *providing feedback on positioning performance*, which helps refine location estimates and improve system robustness [44–47]. From a user intervention perspective, feedback mechanisms introduce an additional layer of *active participation*, requiring users to assess their estimated locations and report discrepancies. In [44], users were prompted to validate their computed positions and offer corrections when necessary, either for benchmarking or processing stages. Similarly, [45,46] leveraged user feedback to fine-tune positioning models, reducing localization errors over time. By incorporating such mechanisms, systems can dynamically adapt to environmental changes and improve their learning-based approaches. However, while user feedback enhances system accuracy, it presents scalability challenges. Requiring manual validation imposes a burden on users, which may lead to low participation rates. Additionally, user-provided feedback can introduce errors if users are not attentive or motivated to provide accurate corrections.
2. Following Instructions: In some crowd-powered IPS, users contribute data by following *simple instructions*, such as walking along predefined paths while their smartphones collect sensor data. This approach is employed in studies like [48–50], where structured user movements are leveraged to improve the accuracy of radio maps. From a user intervention perspective, this method introduces a high level of *active user involvement*, as participants must consciously follow movement guidelines. Unlike fully passive approaches, where data collection is entirely autonomous, these methods require a certain level of user commitment. The quality of the collected data depends on users correctly following the predefined routes, ensuring the coverage and reliability of the generated radio maps. To enhance participation, interactive interfaces should be provided and designed to guide users through the process [48,50]. The role of these interfaces is to provide real-time feedback, navigation assistance, or gamified elements to maintain user engagement. However, despite these enhancements, the requirement for users to physically follow instructions can limit scalability, as sustained participation may decline over time without incentives.
3. Image Capturing and Visual Sensing: Camera-based positioning has been explored in approximately 7 % of existing crowd-powered IPS [51,52]. The integration of camera images with Wi-Fi RSS enables the construction of a radio map, enhancing the accuracy and mitigating thermal heading drift with long-term operations. Studies such as [53,54] have extended this approach by combining camera images with inertial sensors [55], improving robustness in dynamic indoor environments. Further advancements include the integration of a barometer for 3D positioning [56] and the use of magnetic field data [57,58] to enhance localization accuracy. From a user intervention perspective, camera-based approaches generally require *active user participation*, as users must capture images or videos to contribute data. This level of involvement presents scalability challenges, as users may not consistently engage with the system on a large scale. However, some studies have explored methods that rely solely on camera images without Wi-Fi RSS, offering alternative positioning techniques based on AI and image recognition [59–63]. Additionally, camera-based IPS has been integrated with other sensor modalities, such as the magnetic field [32] and BLE RSS [64], reducing dependence on any single sensing method. Despite its potential for high accuracy, camera-based IPS faces practical limitations due to the *requirement for user intervention* in image capture, potential privacy concerns, and increased computational demands for processing visual data. Unless utilized as opportunistic sensing, where data is collected passively while users already use the camera for other purposes, camera-based systems that require *intentional and deliberate user actions* are less suitable for fully autonomous and scalable crowd-powered IPS implementations.
4. Scanning QR Code: Studies [65] have proposed QR codes encoded with deployment location information because they offer low-cost solutions with high positioning accuracy. From a user intervention perspective, QR code-based positioning requires *explicit user actions*, as individuals must physically locate, scan, and interact with QR markers to retrieve or submit location-related data. This level of *manual effort* aligns with *active crowdsourcing* principles, where participants play a direct role in data collection. However, despite the manual intervention required, QR codes provide a low-cost and highly accurate location-labeling solution, which is crucial for maintaining high-quality radio maps. In large-scale crowd-powered IPS, their effectiveness hinges on user adoption rates-frequent scanning improves the density of collected data. Yet, this reliance on users also introduces scalability challenges, as coverage is limited to locations where users actively engage with the system. From an opportunistic sensing perspective, QR codes could be integrated into hybrid models where users naturally interact with them during everyday activities (e.g., payments, navigation). This would reduce the need for **intentional** engagement while still leveraging opportunistic data contributions. However, in their current form, QR-based IPS solutions lean heavily on active rather than opportunistic participation.

3.2.2. Advantages and limitations

Regarding the ***advantages***, prompting users to annotate and localize the indoor fingerprints can ensure a certain level of reliability when experienced users are involved [66]. Providing specific instructions and

proper motivation can further enhance the quality of the contributed data [67]. In direct terms, the primary advantage lies in ensuring the reliability of generated offline databases, such as radio and magnetic maps. However, it is inherently constrained by the level of experience of the participated user [68,69]. As for the ***limitations***, explicit participation-such as providing feedback or manually annotating data-demands active user engagement, which often results in fatigue and declining participation over time. Motivating users in active schemes can be both challenging and costly [70], particularly for tasks requiring frequent input or detailed annotations [71]. Tasks that interrupt users, such as uploading images or adhering to strict instructions, can cause dissatisfaction [72]. Consequently, scalability is inherently constrained, as user compliance, availability, and engagement play critical roles in determining the geographic and temporal coverage of data collection.

3.3. Passive and opportunistic crowdsensing

Generally, opportunistic and passive crowdsensing represent two distinct paradigms in large-scale data collection. Opportunistic crowdsensing relies on context-aware triggers to collect data automatically when specific conditions are met, such as detecting potholes using smartphone sensors during a drive, thereby optimizing resource usage and minimizing user involvement [78]. In contrast, passive crowdsensing involves continuous, unobtrusive data collection, often without explicit user interaction, as seen in wearable devices that persistently monitor health metrics like heart rate [79]. While opportunistic methods prioritize energy efficiency and data quality through techniques like deduplication and collaborative filtering [78], passive approaches often face challenges related to resource inefficiency and heightened privacy concerns due to uninterrupted monitoring [80]. Both paradigms have unique properties; understanding these differences is crucial for designing scalable, ethical, and efficient crowdsensing systems.

3.3.1. Studies adopted opportunistic sensing

Most studies related to crowd-powered IPS have adopted passive user interaction schemes. Despite, several studies employ ***opportunistic sensing*** to construct Wi-Fi radio maps by leveraging data generated as a byproduct of user activities to provide location-labeled Wi-Fi RSS fingerprints, such as NFC/RFID-based payments [73–75], and home/office address tagging [76]. These strategies significantly reduce the burden on users while enabling large-scale, cost-effective radio map construction. However, they introduce challenges such as data sparsity, potential inaccuracies, and dependency on transaction density.

3.3.2. Advantages and limitations

The advantages of this approach can be summarized as follows. This approach is less disruptive, as it can be seamlessly woven into people's daily routines without intruding on their normal activities [66], which boosts scalability and coverage. Additionally, this approach naturally keeps costs down by eliminating the incentives or rewards that active methods often require. While passive methods offer certain advantages, they are also accompanied by several ***challenges*** that must be addressed. Implicit user participation or lack of explicit involvement, including background sensing, raises ethical and privacy concerns if the processes of data collection are not transparent [81]. Therefore, strict policies for data collection and robust encryption mechanisms must be implemented to ensure the security of user data. The other major limitation is accuracy and reliability concerns [82]. The design of automated systems typically requires or favors passive data collection schemes, which, however, do not always fulfill the system's intended promises (especially for the accuracy and reliability metrics) and often underperform in dynamic or noisy environments.

Table 4
Comparison of user involvement types, tasks, and their associated trade-offs in crowd-powered IPS.

Action Type	User Task	Studies	Effort Required	Data Accuracy	Role of User Experience	Scalability
Active	Providing Feedback	[44–47]	Exhausted (Users manually validate location estimates)	User corrections can enhance accuracy	Requires understanding of positioning errors	Limited (User fatigue affects participation)
	Following Instructions	[48–50]	Exhausted (Users follow predefined paths)	Structured data collection can improve reliability	Basic movement guidance is sufficient	Limited (Requires voluntary participation)
	Scanning QR Codes	[65]	Moderate (Users scan QR codes at predefined locations)	Tagged location data improves accuracy	Minimal experience required; simple scanning process	Limited to the existence of QR code and engagement
	Capturing Images	[51–53,57,58,60]	Exhausted (Users must manually take photos)	High (Rich environmental data for localization)	Accurate if users take proper framing and positioning	Limited (Privacy concerns and user effort)
Opport- unistic	Mobile Payment Transactions	[73–75]	Low (Data extracted from transactions)	Moderate (May introduce noise due to lack of validation)	No experience needed; payment is routine	High (No extra effort from users)
	Users' Home or Office Address	[76]	Low (Address linking)	May introduce noise due to lack of validation	No experience needed	Depend on the willing of users to contribute
Fully Passive	Background Crowdsensing	Most other studies, e.g., [8,77]	User only consents once	Dependent on sensor noise and data uncertainties	System operates without user intervention	Very High (Runs automatically in the background)

Table 5
Summary of quantitative impact of user interventions on positioning accuracy.

Intervention Type	Study	Accuracy Results	Methodology Highlights
Active Via Image Capturing	Dong et al. [56]	Location error: 1m; Facing direction error: 6∘	SfM-generated 3D models, OCR for POIs, barometric sensing for multi-floor navigation.
	Liu et al. [53]	Geo-tagging error: 0.67m Trajectory error: 0.6–1.56m Wi-Fi RSS localization error: 3.2 m. Image-matching localization error: 1.2m	Visual-inertial geo-tagging, minimal manual reference points, sliding-window filter, trajectory reconstruction via inertial and visual data fusion.
Active Via Scanning QR Code	Wan et al. [65]	Localization error reduced from 2.4m (forward EKF) to 1.2m (backward EKF smoothing)	User scans QR codes to anchor trajectory points, employing EKF smoothing techniques for improved accuracy.
Active Via Providing Feedback	Guo et al. [45]	11.9 % step-level navigation error Effective navigation without physical maps or infrastructure	Users identify landmarks (e.g., signs, room numbers); virtual paths are constructed from Wi-Fi fingerprints linked to these landmarks; real-time instructions guide users via recognized landmarks.
	Li et al. [47]	Mean error reduced from 3.2m to 2.2–2.5m after anomaly filtering; TPR/TNR up to 95 %	Users submit RSS data with pseudonyms; ACTD filters abnormal data using rarity scoring, sequence modeling, and metric learning to improve localization robustness and accuracy.
	Li et al. [46]	Maintains over 80 % room-level accuracy after 1 week; More than 60 % accuracy under 80 % malicious correction rate	Users can approve or correct estimated positions; accepted corrections update the fingerprint DB via DBSCAN-based clustering to filter errors; robust to environment and attacker input.
Active Via Follow Instructions	Santos et al. [49]	Mean positioning error: 2.3m (office) and 4.7m (university) with crowdsourced fingerprints	Users followed pre-defined paths to collect multimodal data (Wi-Fi, magnetic, inertial); trajectories were fitted using particle filtering with floor plan constraints; evaluation showed comparable or better results than traditional fingerprinting in office environments.
	Radu and Marina [50]	Median error: less than 3m (multi-floor). Under 2m (phone in hand, single floor)	Users follow predefined paths across stairs, elevators, and corridors; system fuses activity-aware PDR with selectively weighted Wi-Fi fingerprints via a particle filter; minimal building layout required.
Passive (Background Sensing)	Liu et al. [77]	Average localization error: 2–3 m (indoor); seamless transition across indoor-outdoor environments	System uses multimodal features (Wi-Fi, GPS, cellular, magnetic field, barometer) with fingerprint reuse and automatic mode switching to support robust city-scale indoor-outdoor positioning.
	Gu et al. [83]	Mean error at landmarks: 3.6m; 80 % of test errors under 10m with crowdsourced RM	Combines foot-mounted IMUs, GPS, and Wi-Fi RSS using graph-based SLAM; constructs trajectories and crowdsourced RM for FWIP without active user involvement; GPS provides spatial anchors to align and calibrate DR and RSS observations.
Opportunistic (Mobile Payment)	Ahn and Han [74]	Positioning error reduced from 9.9 m to 6.8 m via crowdsourced refinement	Initial radio map built using Wi-Fi fingerprints collected during mobile payment transactions; improved via HMM-based location-labeling and optimization of reference locations using genetic algorithms. Evaluated in three large malls.
	Zhou et al. [75]	Classification accuracy: 91 % at shop-level. Outperforms LR, AdaBoost, XGBoost baselines	Uses Wi-Fi RSS collected during mobile payment transactions; applies CNN-based joint training on RSS and shop metadata using a sliding window of 1–23 days; achieves high-precision shop identification in malls with minimal user effort.
Opportunistic (Address-based Tagging)	Han et al. [76]	Avg. error: less than 10 m at 50–60 % collection rate (except Galleria: 20 m). Outperforms Google WPS (less than 25 m) indoors	Users' home/office addresses used for fingerprint tagging; clustering and geocoding applied to enable GPS-free indoor localization; scalable to city-wide deployments with passive background collection.

3.4. Quantitative assessment for the impact of user intervention on system performance

The extent and nature of user intervention in crowd-powered IPS have a significant impact on system performance, particularly in terms of positioning accuracy. This subsection presents a quantitative assessment of positioning accuracy as influenced by various user intervention strategies, as summarized in Table 5.

Among the most accurate systems are those that rely on image-based localization, where users actively capture visual data during navigation. These methods leverage smartphone cameras and inertial sensors to construct 3D environmental models and perform precise localization. For instance, the ViNav system [56] achieves a location error of less than 1 meter and an orientation error below 6 degrees by using Structure-from-Motion (SfM) techniques combined with barometric sensing and optical character recognition. Similarly, Liu et al. [53] report a geo-tagging error of 0.67 meters and trajectory reconstruction errors ranging from 0.6 to 1.56 meters by fusing visual and inertial data through sliding-window filtering. These results highlight the potential of visual sensing to achieve sub-meter localization accuracy in indoor environments.

Other forms of active participation, such as scanning QR codes, also yield high localization precision. Wan et al. [65] demonstrate that by anchoring user trajectories through QR code scans and applying backward Extended Kalman Filter (EKF) smoothing, the average localization error can be reduced from 2.4 meters to 1.2 meters. This illustrates how simple user tasks can significantly enhance position ing fidelity when combined with temporal filtering methods.

Feedback-based systems, where users validate or correct estimated locations, demonstrate moderate to high positioning accuracy depending on the feedback mechanism and aggregation method. The FreeNavi system [45], which uses user-identified landmarks to construct virtual paths, reports a step-level navigation error of 11.9 %, enabling mapless and infrastructure-free navigation. ACTD [47], which incorporates feedback through crowdsourced RSS data, reduces the mean error from 3.2 meters to a range of 2.2 to 2.5 meters by filtering anomalous data using rarity scoring, sequence modeling, and metric learning. Additionally, Li

et al. [46] maintain over 80 % room-level accuracy for a full week post-deployment and demonstrate resilience under adversarial conditions, preserving more than 60 % accuracy even when 80 % of user corrections are malicious. These results affirm the value of user feedback in both enhancing positioning robustness and detecting abnormal contributions.

Another category of active user involvement involves following structured paths or predefined instructions during data collection. These systems guide users through specific trajectories to ensure spatial diversity and coverage. Santos et al. [49] report a mean error of 2.3 meters in an office setting and 4.7 meters in a university environment using particle filtering over multimodal data. Likewise, HiMLoc [50], which combines activity-aware pedestrian dead reckoning with selective Wi-Fi fingerprinting, achieves a median localization error below 3 meters in multi-floor buildings and under 2 meters for single-floor use cases with handheld devices. Such systems demonstrate the value of structured mobility in enhancing localization precision while maintaining practical deployment requirements.

In contrast to active strategies, opportunistic approaches minimize user burden by leveraging ambient data sources. Ahn and Han [74] demonstrate that by collecting Wi-Fi fingerprints during mobile payment transactions and refining them through HMM-based optimization, localization error can be reduced from approximately 9.9 meters to 6.8 meters. Zhou et al. [75] employ a convolutional neural network (CNN) trained on Wi-Fi and purchase metadata to achieve 91 % shop-level classification accuracy, demonstrating the potential of machine learning in sparse-label environments. Meanwhile, Han et al. [76] introduce an address-based method that uses users' home and office locations to tag indoor Wi-Fi signals. This approach achieves an average error below 10 meters when at least 50–60 % of household data is collected, significantly outperforming traditional Wi-Fi Positioning Systems (WPS), such as Google's, which exhibit 5–25 meter indoor errors.

Beyond opportunistic use cases, passive strategies further minimize user burden by enabling background data collection without any explicit user interaction. A prominent example is SoiCP [77], a seamless outdoor-indoor positioning system that leverages multimodal sensor data, such as GPS, Wi-Fi, cellular signals, magnetic field, barometric pressure, and user activity, collected opportunistically during natural user mobility. SoiCP achieves competitive indoor localization accuracy (approximately 2–3 meters) through intelligent fingerprint reuse and adaptive indoor-outdoor switching. Similarly, Gu et al. [83] demonstrate a passive framework for trajectory estimation and radio map construction that combines foot-mounted inertial sensors, Wi-Fi RSS, and GPS signals. Their system uses graph-based SLAM to align dead reckoning and fingerprint observations, achieving a mean error of 3.6 meters at landmarks and keeping 80 % of localization errors under 10 meters. Crucially, the effectiveness of such passive approaches is largely enabled by the availability of external calibration resources, such as accurate GPS data near building entrances and semi-outdoor regions. These calibration anchors serve as spatial references for associating environmental fingerprints with ground-truth positions, thereby compensating for the absence of active user involvement. This highlights that while passive systems eliminate manual effort, their performance remains contingent on the presence and consistency of ambient calibration signals.

Taken together, these results reveal a clear performance spectrum across user intervention strategies in crowd-powered IPS. Systems requiring high user involvement-such as those based on visual sensing, structured trajectory following, or direct feedback-consistently achieve the highest localization accuracy, typically ranging from 0.6 to 2.5 meters. Feedback-based and instruction-guided systems generally perform in the 2–3 meter range, balancing moderate user effort with reliable data quality. Opportunistic approaches, including those that leverage mobile transactions or inferred address-based tagging, enable scalable deployment with minimal user burden, though often at the cost of reduced accuracy, typically falling in the 6–10 meter range. Passive systems have recently demonstrated the potential to narrow this gap, although their performance exhibits a wide spectrum of error that largely depends on the availability and accuracy of calibration resources. These resources are themselves influenced by contextual factors such as the building's location and its surrounding environment, similar to the situational dependencies observed in GNSS-based systems.

These findings underscore a fundamental trade-off between localization precision and the level of user effort required. They offer practical guidance for selecting IPS strategies based on application requirements, deployment scalability, and acceptable accuracy thresholds. In particular, while active user interventions can substantially enhance positioning performance, well-designed passive or opportunistic systems-when supported by robust calibration mechanisms-can provide accurate and scalable alternatives. Analyzing positioning accuracy metrics enables a meaningful quantitative comparison across user involvement schemes. However, it is important to recognize that direct comparisons may be influenced by various external factors, including environmental complexity, device heterogeneity, signal density, and the availability of ground truth for calibration, as follows:

- Environmental conditions (e.g., building layout and size)
- Deployment characteristics (e.g., number and distribution of APs)
- Availability of additional calibration resources (e.g., GNSS conditions surrounding the building, floor plans, and sensor fusion)

Future research should include dedicated quantitative comparison studies that experimentally evaluate the effects of user involvement on positioning accuracy. To ensure fair and reliable comparisons across different indoor environments and deployment conditions, such studies should normalize key variables to mitigate confounding factors.

Regarding the quantitative impact of the type of user intervention on data volume and scalability: User willingness to engage with the system has a direct influence on both the volume of collected data and the scalability of crowd-powered IPS, in both the short and long term. Unlike positioning accuracy, which can be objectively measured against ground truth, scalability and user engagement must be assessed through indirect means, such as user surveys or behavioral analysis derived from system logs. One promising approach is the use of structured questionnaires to evaluate user acceptance, perceived burden, and willingness to participate under different data collection modalities. These surveys can be embedded unobtrusively into positioning or navigation applications, presented as short and time-sensitive prompts during use. However, such practices remain largely underexplored in current crowd-powered IPS implementations, representing a valuable direction for future research.

In another way, quantitative indicators, such as participation rate, response frequency, and session duration, can be extracted from system usage logs to infer user engagement levels. Additionally, fuzzy logic-based models or multi-criteria decision-making (MCDM) approaches (e.g., AHP, TOPSIS) can be employed to synthesize multiple qualitative factors into a numerical index that represents user acceptance and scalability. Given the significant impact of incentives on user involvement, they should be excluded from the assessment to ensure a pure evaluation of how different types of user participation influence acceptance, data volume, and scalability. By isolating the effects of user involvement from external motivational factors, a more unbiased understanding of the inherent willingness to contribute can be obtained, providing clearer insights into the feasibility and sustainability of various participation schemes. Notably, privacy concerns play a critical role in shaping user willingness to participate in data collection tasks. To ensure reliable assessments of scalability and engagement, it is essential to declare to the participants the trust mechanisms that guarantee data security, anonymity, and transparent handling policies. Without such assurances, users may hesitate to contribute, leading to biased participation rates and potentially compromising the reliability of scalability evaluations. Additionally, a comparative analysis of participation rates before and after implementing privacy-enhancing techniques should be conducted to quantify their impact on user willingness to participate and system scalability. This approach enables cross-validation of how differ-

Table 6
Comparison between active and passive user involvement schemes.

Aspect	Active User Involvement	Opportunistic or Passive User Role
User interaction and control	Users actively engage in the system by data collection and providing feedback or any type of active participation.	No user intervention is required; only user approval is needed for crowdsourcing.
Coverage and scalability	User acceptance and participation limit it.	Offers broader geographic and temporal data coverage.
User intrusiveness	Potential interruption to user tasks due to active engagement.	Minimizes user burden and interruptions.
Experience level	Experienced users can offer a reliable solution and mitigate database uncertainty.	Less practical; alternative resources replace user involvement.
Cost and Incentives	May incur higher costs due to demands for incentives.	Cost-effective; mitigates the need for incentives.
Vulnerability to jamming and fake participation	Vulnerable to misinformation or fake contributions.	Less susceptible to deliberate false data inputs or attacks.
Security and privacy control	Requires explicit instructions, transparent measures, and clear incentives.	Requires strong privacy safeguards, user consent, and robust encryption protocols.
Human-centricity and automation	Fosters human-centric interaction for nuanced data collection.	Relies on automated methods, reducing human intervention.
Self-deployable development and ubiquity	More challenging due to reliance on user input and engagement.	Easier due to reduced user dependency.

ent user involvement schemes and privacy-preservation measures influence engagement levels, ensuring a more comprehensive assessment of the trade-offs between data protection and participatory scalability. By integrating experimental evaluations, user surveys, and statistical modeling, a more comprehensive quantitative assessment of user involvement in crowd-powered IPS can be achieved. These analyses provide valuable insights into how different user participation schemes influence system performance and adoption.

3.5. User involvement choice: Dilemmas & trade-offs

As evidenced by the preceding qualitative and quantitative analyses, the decision to adopt active, opportunistic, or passive user participation in crowd-powered systems involves navigating several critical trade-offs, notably those related to scalability, data reliability, operational cost, and security concerns [84,85]. Awareness of these trade-offs guides systems design toward effectively balancing user engagement with operational performance. A detailed comparison of these approaches is shown in Table 6.

1. *Scalability vs. Data Reliability (Automation vs. Human Centricity)*: Passive user involvement, which implies limited interaction and uses automated data collection, is efficient in scalability and ease-of-use [86]. It can be seamlessly integrated into users' daily routines, thus enabling broad geographic and temporal coverage with a minimum need for active user interaction. This often comes at the cost of data reliability because they lack the depth expert users provide. On the other hand, active user involvement improves data reliability by leveraging user expertise and focused contributions. This is a good method for generating high-quality offline maps of radio or magnetic fields. However, active user involvement poses scaling challenges because the coverage in both participants and geography is contingent upon user availability and willingness [87].
2. *Cost vs. Scalability and Quality*: Active systems rely on incentives that motivate users to participate, making them operationally expensive [88]. However, despite these costs, such incentives return benefits in terms of better data quality and the possibility to target underrepresented or unpopular areas. Passive systems, on the other hand, avoid any incentive mechanisms and are thus more cost-efficient and easily scalable [89]. In this case, such cost-efficiency comes with a price: lack of control over data quality and reduced adaptability to concrete requirements [90].
3. *Security, Privacy, and System Vulnerabilities Vs Quantity*: Passive systems raise a big question in privacy due to continuous background data collection; thus, users are not always aware of what happens with their data. Such issues could be handled by proper encryption and clear policies regarding data to keep users' trust intact [81]. Whereas, active systems have more transparency in their processing, and user controls can easily be exercised which help to reduce privacy risks. However, they tend to be very vulnerable in cases of fake participation, misinformation, or abuse of incentive mechanisms, and even hacking and malicious attacks [91].

Analyzing these trade-offs provides valuable evidence of the strong interconnection between user-related issues and the design objectives of crowd-powered IPS systems. By highlighting these relationships, we can better understand how user participation choices significantly influence system scalability, data reliability, cost, and privacy. This analysis not only helps in clarifying the inherent challenges but also builds the foundation and justification for the recommendations outlined in Section 7. These recommendations are designed to address these trade-offs effectively, ensuring a balanced and user-centric approach to system design.

3.6. Concluding remarks

The analysis of active, opportunistic, and passive user participation in crowd-powered IPS highlights the inherent trade-offs between scalability, accuracy, cost, and privacy. Active participation generally yields higher positioning accuracy and richer contextual data but suffers from scalability and long-term engagement challenges. Opportunistic and passive approaches improve coverage and reduce user burden, yet they often require supplementary mechanisms to maintain data quality and reliability. These dynamics underscore the central role of user engagement in shaping system performance and sustainability. Consequently, understanding and addressing the factors that motivate user participation becomes essential. The following section explores incentive mechanisms as a critical driver for attracting and retaining contributors in crowd-powered IPS.

4. User incentives in crowd-powered IPS

A critical limitation of MCS-based IPS lies in their dependency on sustained user participation. Without a sufficiently large and continuous participant base, data collection campaigns risk producing insufficient coverage and temporal continuity, leading to rapid degradation of system accuracy and reliability. This challenge is particularly acute in long-term deployments, where participant fatigue and declining engagement can undermine the viability of the system. Therefore, recruitment strategies must be complemented by mechanisms for ongoing motivation and retention to ensure the continuous flow of high-quality data.

Consequently, incentive mechanisms play a crucial role in stimulating user participation in crowd-powered systems by addressing diverse user needs and aligning them with system objectives [70,72].

This section provides a comprehensive review of user incentives in crowd-powered IPS, structured as follows. First, we examine the underlying user motives and categorize the types of incentives commonly employed in MCS applications. Next, we explore the utility functions associated with these incentives and their interaction with pricing models. This is followed by an investigation of the technologies used for incentive modeling and the key considerations in designing and implementing incentive mechanisms in real-world applications. Subsequently, we highlight the differences between incentives in the IPS field and other crowd-driven domains, analyzing IPS-specific objectives associated with employing incentive mechanisms. Finally, we review existing incentive mechanisms in crowd-powered IPS, focusing on their mathematical formulations, before conducting a quantitative assessment of these mechanisms and identifying key shortcomings and gaps in current approaches.

4.1. Types of incentive mechanisms

Crowd-powered systems, including crowdsourcing and MCS, leverage the contributions of a large number of users (e.g., smartphone owners) to perform sensing tasks or solve human-intelligence problems. Ensuring sufficient participation and quality is a core challenge because users incur effort, time, and potentially privacy costs when contributing data. Consequently, the design of effective **incentive mechanisms** is essential to sustaining user engagement and maintaining data quality.

This gives rise to a fundamental question: *Why do individuals choose to participate in crowd-powered platforms?* Fig. 7 presents a taxonomy of common user motives along with the associated incentives for each motive. Broadly, motivations fall into two categories. Some individuals are driven by **intrinsic motivations**, such as the enjoyment of helping others, the pursuit of personal development, or the satisfaction derived from learning new skills [92]. For example, platforms like Duolingo harness intrinsic incentives through gamification and progress tracking, appealing to users' desire for self-improvement and achievement [72]. In contrast, other users are motivated by **extrinsic drivers**, including financial rewards, recognition, or career advancement opportunities [70,72]. Amazon Mechanical Turk, for instance, employs reputation systems to promote high-quality task completion, while platforms such as Innocentive offer significant monetary rewards for solving complex problems [72,93].

A widely used taxonomy classifies incentives into three categories: **monetary**, **non-monetary**, and **hybrid** models, as shown in Fig. 8. Each category appeals to different user motivations and is strategically applied depending on the nature of the task and the target participant group.

4.1.1. Monetary incentives

Monetary incentives use direct financial rewards to motivate participation. This is the most straightforward approach: participants receive payments (cash, credits, vouchers, tokens, etc.) in exchange for completing tasks or contributing data. Monetary incentives are widely adopted due to their versatility and ease of implementation [94]. Key models include:

- **Fixed Payments**: Each task has a predetermined reward. Fixed pricing is simple and guarantees a known reward for participants, which can attract users seeking assured compensation. However, setting the reward level is critical, too low may fail to attract enough workers, while too high could waste the budget. A pricing analysis on *TopCoder* (a software crowdsourcing platform) showed that higher task awards attract more submissions and faster completion [95]. Still, beyond a point, they did not always improve solution quality.
- **Auctions (Dynamic Bidding)**: Auction-based incentives treat the reward determination as a market mechanism. In a reverse auction setting, the platform (task requester) announces a task, and participants bid the minimum price at which they are willing to do it. The platform then selects winners (e.g., lowest bids) and pays them, often using a second-price or Vickrey scheme to ensure truthfulness. Auctions can improve cost-effectiveness by leveraging competition – the platform pays just enough to get the required workers. For instance, Wen et al. [96] propose a quality-driven auction where payments depend on data quality, the system pays workers based on their contributed sensor data quality, and proves the auction achieves optimal social welfare while being truthful and individually rational. Auction models can be highly effective in cost control, but they introduce complexity for users (who must understand how to bid). They may deter participation if the process or outcome seems unfair (e.g., only the lowest bidders get paid). To mitigate this, some systems use simplified auctions or contest formats to preserve incentive compatibility without burdening users.
- **Dynamic Pricing**: Rather than a one-time reward determination, dynamic pricing adjusts incentives over time or based on supply-demand conditions. In online crowdsourcing scenarios where tasks and users arrive continuously and unpredictably, the platform can employ dynamic pricing strategies to meet participation targets [94]. For example, if initial offers fail to attract enough contributors for a sensing task, the platform may incrementally raise the reward until the required number of users is accepted, analogous to surge pricing. Conversely, for oversubscribed tasks, it might lower payments or select the cheapest bidders. Dynamic pricing often relies on real-time algorithms or rules. Gao et al. [97] model a point-to-point dynamic crowdsensing problem as a two-stage Stackelberg game and derive how the optimal task price should change with the current supply of sensors and demand for data [98]. These strategies require careful design to avoid oscillations or user dissatisfaction. Nonetheless, dynamic monetary incentives can improve efficiency by allocating the budget where and when needed most and by adapting to user behavior on the fly. Machine learning approaches are more suited for this category to fine-tune prices based on past responses.

Beyond these, other monetary incentive schemes include contest rewards (prize-based competitions where only top performers win a large reward) and bonus payments for high-quality work. Contests can stimulate effort through competition but might discourage those who frequently lose. Overall, monetary incentives directly leverage extrinsic motivation (financial gain) and have been the focus of extensive research because they are tangible and universally valued. Most real-world crowdsourcing platforms (Amazon Mechanical Turk, ride-sharing services, etc.) rely on monetary payments as the primary incentive.

4.1.2. Non-monetary incentives

Non-monetary incentives motivate users through rewards that are not financial. These mechanisms aim to harness intrinsic or social motivations:

- **Gamification (Entertainment)**: Tasks are designed as games or made fun via points, badges, leaderboards, and challenges. By turning contributions into a game-like experience, users participate for enjoyment and competition rather than just a paycheck [99]. For example, a crowdsensing app might present environmental data collection as a treasure hunt or a friend competition. Early work in this vein created sensing games where users perform sensing tasks implicitly while playing (e.g., a location-based game that incidentally collects GPS traces). It has been used successfully in some domains (e.g., Foldit for protein folding or mapping games) and can lead to high user engagement. However, designing an effective gamification scheme requires creativity and task-specific customization. Not all tasks are easily gamified, and poorly designed games may fail to retain interest. Nonetheless, when applicable, gamification can reduce the need for monetary payments by providing intrinsic rewards (enjoyment).

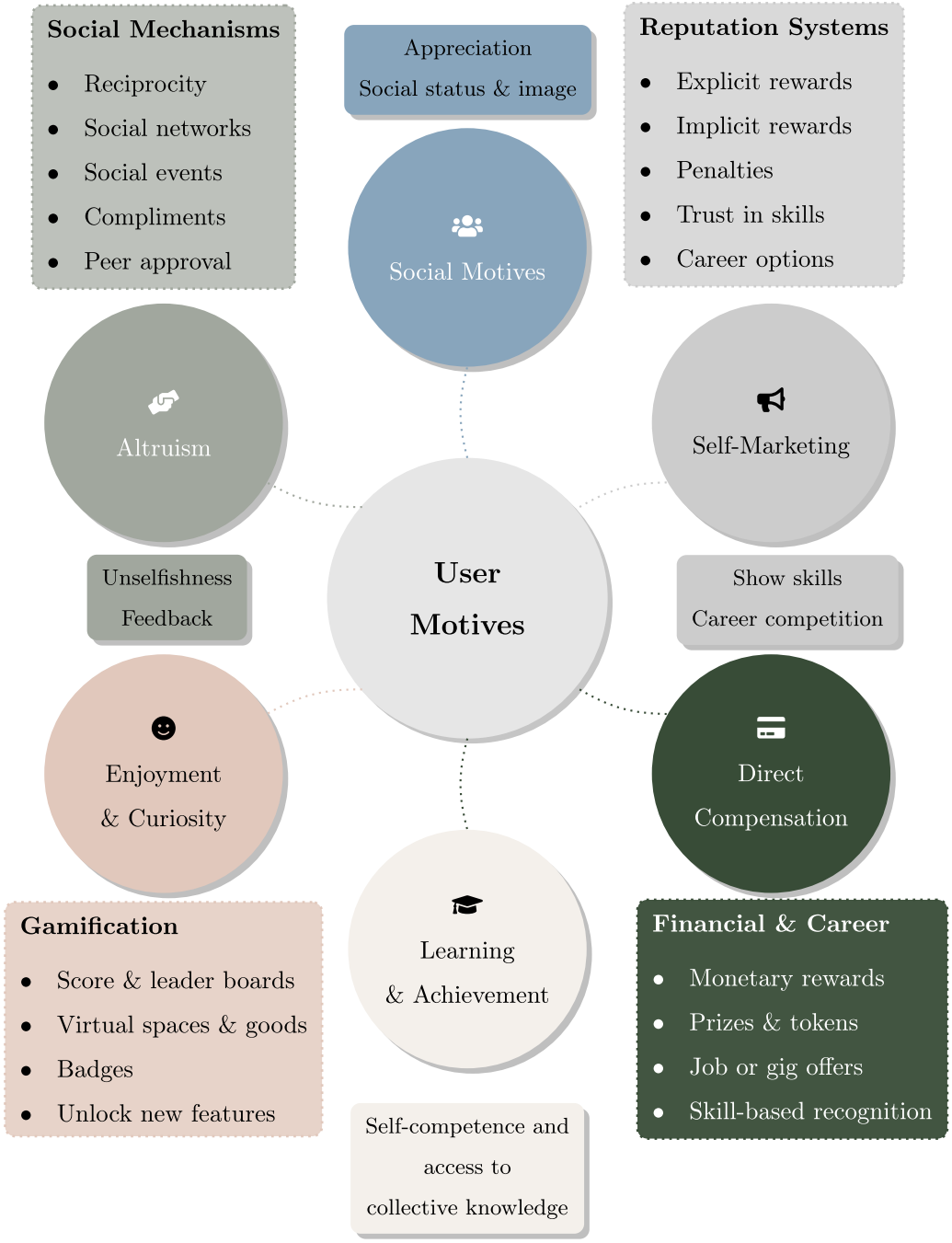

Fig. 7. A taxonomy of user motives and incentive mechanisms in MCS, with the combination of different categories (hybrid mechanisms).

- **Reputation and Social Recognition**: Many crowdsourcing systems employ reputation points, ratings, or badges as incentives. Contributors earn a score or level for each task completed, which is visible to the community or unlocks privileges. A high reputation can bring intangible benefits: recognition as an expert, increased trust, or access to more opportunities. For instance, Q&A platforms like Stack Overflow reward users with reputation points and badges for good answers, incentivizing continued contributions. In mobile crowdsourcing, a sensing platform might rank participants by reliability or data quality, motivating them to maintain a good standing. Reputation systems serve both as motivation and quality control (since users want to avoid bad ratings). Research has shown that reputational incentives can reduce free-riding and false reporting [100]. However, reputation only motivates those who value the platform's community or future rewards; new users or those less interested in status may not respond as strongly. There is also a risk of gaming the reputation system unless carefully designed.
- **Altruism and Civic Incentives**: Participants can be driven by social good, community belonging, or personal satisfaction rather than material reward. In crowdsensing for civic or environmental causes, people may contribute out of altruism or civic duty (e.g., reporting pollution levels to help the community). Platforms can reinforce this by highlighting the social impact of contributions or providing social feedback – for example, showing contributors that their data was used in a public map or acknowledging top volunteers in a community forum. Social incentives also include peer encouragement and competition: integrating crowdsourcing with social networks, allowing users to share contributions or form teams, can spur participation

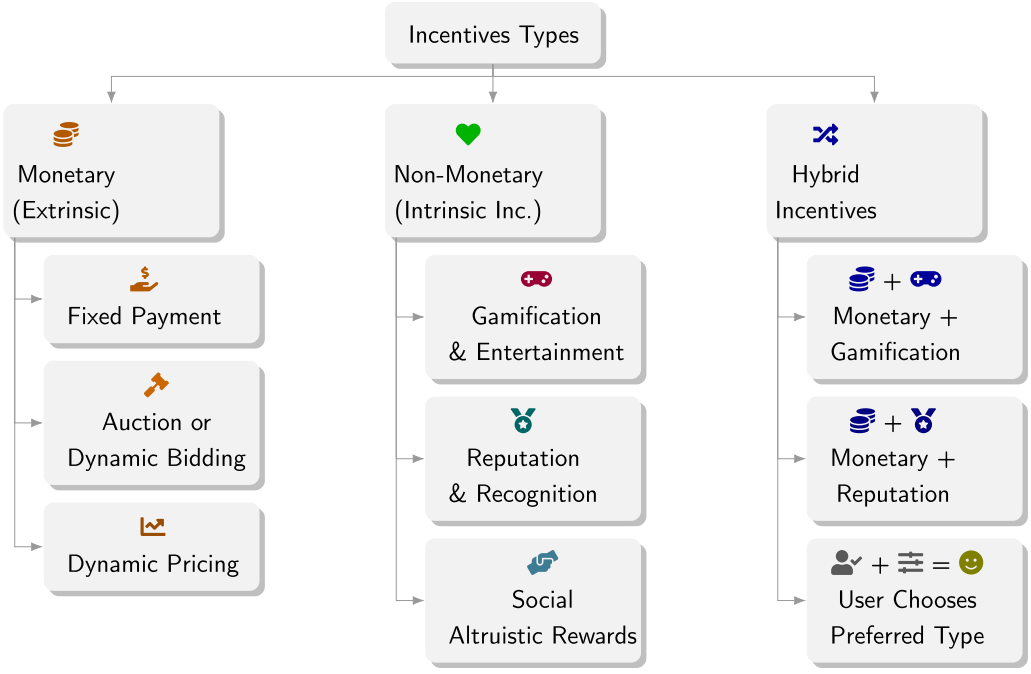

Fig. 8. Taxonomy of incentive mechanisms in MCS: Monetary mechanisms based on extrinsic drivers, non-monetary mechanisms based on intrinsic motivations, and the integration between them.

through peer recognition. Some systems offer non-monetary perks like titles (*Community Ambassador*) or opportunities to be featured in newsletters, which reward participants with public recognition. These incentives leverage intrinsic motivations (like altruism, curiosity, or desire for social approval). They tend to be context-dependent – effective mainly if contributors genuinely care about the mission or community. One challenge is sustaining long-term engagement purely through intrinsic motivation; as tasks become routine or burdensome, participation might wane without additional rewards [99].

- **Service Exchanges**: Another non-monetary model is a barter or service exchange principle: users are rewarded with services, privileges, or resources in return for their contributions [33]. For example, a participatory sensing application might offer improved application features, extra storage, or premium access to data analytics for users who contribute data. This follows a mutual benefit idea – "you help me collect data, I give you some service or benefit in return." In networks of peers, this could mean reciprocal task solving (users solve each other's tasks). An illustration is traffic apps like Waze, where users report road conditions and, in exchange, gain access to real-time traffic data improved by everyone's contributions. Here, the service (better route recommendations) acts as the incentive. Service-based incentives avoid direct payments and can be efficient if the provided service has a low marginal cost. However, they only work when the platform can offer something the users value in return. Designing a fair exchange rate (how much service per contribution) and ensuring perceived fairness is important to keep participants motivated.

Non-monetary incentives are powerful in that they can harness intrinsic motivation, potentially leading to more sustainable engagement (users contribute because they want to, not just for money). They also avoid the monetary costs and complexities of payments. However, they are often task-specific and user-specific; what works as a fun incentive in one context might not translate to another. Many successful crowdsourcing efforts thrive on non-monetary incentives (like community and purpose), but monetary incentives might be necessary for more tedious tasks or when broad participation is needed quickly. A phenomenon known as *crowding out* is also a concern: introducing payments can sometimes reduce intrinsic motivation (people stop doing it for fun once it becomes *for money*), and similarly, relying only on intrinsic motivation might exclude those who would participate only if paid. This leads to the consideration of hybrid approaches.

4.1.3. Hybrid incentive models

Hybrid incentive models combine monetary and non-monetary rewards to leverage both advantages. The goal is to create a more robust incentive scheme that appeals to a wider range of participant motivations and avoids the pitfalls of using a single type of incentive. The following are examples of hybrid mechanisms:

- **Combining Extrinsic Drivers (Monetary) and Intrinsic Motivations (Non-Monetary)**: There are two main subcategories of this combination. *Monetary with Gamification*: Systems such as Steemit combine token rewards with gamified interfaces. Studies [33] show increased engagement and content quality through dual incentives. *Monetary with Reputation*: Combining pay-per-task with a reputation system ensures short-term and long-term motivation. Reputation may also determine access to higher-paying tasks [94]. However, designing a hybrid incentive mechanism raises its own challenges. The interplay between different incentives must be managed to avoid undermining the other. As noted, offering money can sometimes decrease a person's intrinsic drive if not handled properly. Therefore, platforms need to calibrate how and when each type of reward is given. Fairness and transparency are also key; participants should feel that the combined rewards are distributed justly for their efforts.
- **User Chooses Preferred Type**: Recent work [101] even suggests allowing participants to choose their preferred incentive type. In a field experiment on crowdsourced innovation, allowing solvers to choose between reward types (e.g., money vs. a certificate) led to higher solution quality than a one-size-fits-all incentive because individuals could pick what motivates them best. This underscores that different people respond to different incentives, and a flexible hybrid system can harness that diversity.

In summary, hybrid models can maximize engagement by combining the scalability and direct motivation of monetary payments with the sus-

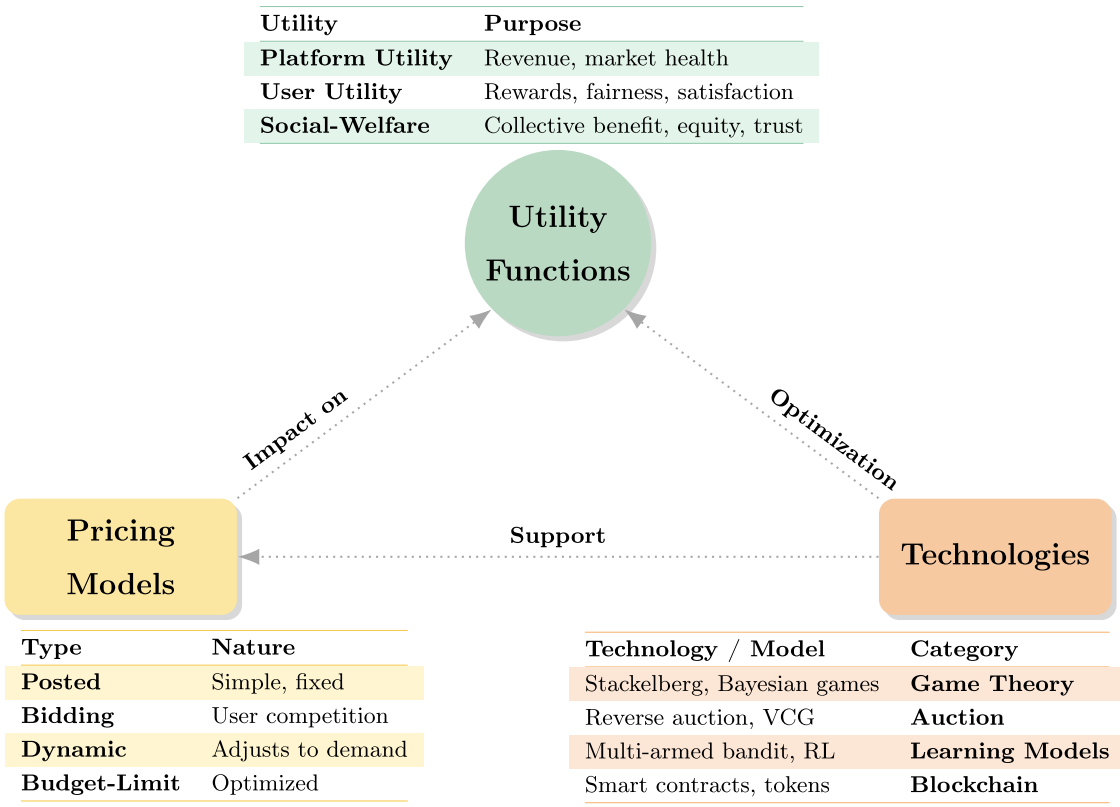

Fig. 9. Interplay between utility functions, technologies, and pricing models in incentive mechanism design (Figure inspired and designed based on the illustration of incentive mechanisms in MCS in [102,103]; augmented with additional stage-wise summary tables to provide a comprehensive overview of the entire incentive design process).

tainability and richness of non-monetary rewards. Subsequent sections examine the technological enablers, theoretical foundations, and practical challenges involved in designing and implementing such hybrid incentive mechanisms.

4.2. Utility functions and pricing models

Understanding the design of incentive mechanisms in MCS platforms requires a structured approach to balancing different objectives. As illustrated in Fig. 9, incentive mechanisms are shaped by three core components: **utility functions**, **technologies**, and **pricing models**. These components interact in a way that influences both platform sustainability and user participation. Fig. 9 visually encapsulates these relationships, providing a conceptual framework for understanding the intricate interplay between these key components. Utility functions represent the core analytical tools within incentive mechanism frameworks, quantitatively characterizing the objectives, preferences, and strategic interactions of stakeholders. These functions are deeply intertwined with pricing mechanisms, shaping their effectiveness and outcomes. The primary utility functions include participant, platform, and social welfare utilities, each interacting with distinct pricing models, as detailed subsequently.

4.2.1. Utility functions

Participant Utility Function: Participant utility functions quantify the net benefit individuals gain from participation, directly influencing their decision-making processes regarding task involvement. Fundamentally, participant i incurs a task-specific cost c_i, encompassing effort, time expenditure, device resource consumption (e.g., battery drain), or privacy costs. In return, the participant receives a reward p_i from the platform. The participant's utility u_i is defined as the net benefit:

$$u_i = p_i - c_i, \tag{1}$$

with the essential individual rationality constraint ensuring participation only if:

$$u_i \geq 0. \tag{2}$$

More sophisticated participant utility formulations explicitly incorporate quality or effort levels. Let $q_i \in [0, 1]$ represent the measurable output quality provided by participant i. The payment then becomes contingent on this quality metric:

$$p_i = R \times q_i, \tag{3}$$

where R represents a base reward set by the platform. Consequently, participant utility evolves into a quality-sensitive function:

$$u_i = Rq_i - c_i(q_i), \tag{4}$$

where $c_i(q_i)$ typically increases with q_i. Participants strategically optimize their chosen quality level q_i^* to maximize utility, subject to incentive compatibility constraints ensuring truthful reporting:

$$u_i(\theta_i) \geq u_i(\hat{\theta} \mid \theta_i), \quad \forall \hat{\theta} \neq \theta_i, \tag{5}$$

where θ_i is participant i's true type or valuation, and $\hat{\theta}$ represents any misreported type.

Platform Utility Function: The platform's utility function encapsulates strategic objectives such as cost minimization, data quality maximization, budget adherence, and operational efficiency. Suppose the platform assigns valuation v_i to each completed task, influenced by quality metrics q_i:

$$v_i = v \times q_i, \tag{6}$$

where v represents intrinsic economic or strategic value derived from high-quality data. The platform's utility thus becomes:

$$U_{\text{platform}} = \sum_{i \in S} v_i - \sum_{i \in S} p_i. \tag{7}$$

Social Welfare Function: This function captures collective stakeholder benefits, fairness, equity, and sustainable engagement:

$$W_{\text{social}} = U_{\text{platform}} + \sum_{i \in S} u_i. \tag{8}$$

4.2.2. Interactions with pricing models

Pricing models mediate between participant and platform utilities, influencing participation rates, task quality, budget efficiency, and system robustness. Notable models include:

- *Posted Pricing:* Offers fixed rewards ($p_i = R$), requiring calibration to achieve equilibrium between participation and efficiency. Participation occurs if:

  $$R \geq c_i. \tag{9}$$

- *Bidding Systems:* Users competitively bid their costs, with the platform dynamically allocating rewards. Incentive compatibility ensures truthful reporting:

  $$u_i(\theta_i) \geq u_i(\hat{\theta} \mid \theta_i), \quad \forall \hat{\theta} \neq \theta_i. \tag{10}$$

- *Dynamic Pricing:* Rewards adapt to fluctuations in demand or participation. The platform sets rewards $p_i(t)$ dynamically to maintain engagement and maximize utility over time, often expressed as:

  $$p_i(t) = f(\text{demand}, \text{participation rate}, t), \tag{11}$$

  where $f(\cdot)$ is an adaptive function adjusting incentives in real-time.
- *Budget-Limited Pricing:* Explicitly integrates financial constraints into the incentive structure:

  $$\sum_i p_i \leq B, \tag{12}$$

  ensuring cost-effective distribution of incentives within a fixed budget, often employing optimization algorithms or auction mechanisms to achieve efficiency, the platform solves the constrained optimization problem:

  $$\max_{\{p_i\}} \sum_i v_i, \quad \text{subject to } u_i(p_i) \geq 0 \quad \forall i, \quad \text{and} \quad \sum_i p_i \leq B. \tag{13}$$

Each pricing model shapes the strategic environment uniquely, directly affecting participant behavior, engagement sustainability, and overall incentive compatibility. Hence, successful incentive design involves selecting and calibrating pricing models aligned with stakeholder utility functions and strategic objectives, ensuring fairness, efficiency, and long-term sustainability.

4.3. Technologies and implementations steps

Various computational and economic models underpin the incentive structures, optimizing how rewards are allocated and ensuring efficient resource distribution. These include the following models.

4.3.1. Game-theoretic modeling

Game theory is the study of strategic interactions among rational decision-makers. In mobile crowdsourcing, one can view the platform and the users as players in a game. Each user decides whether to participate (and how much effort to exert) based on the incentives and their own cost/benefit, while the platform "sets the rules" (payments or rewards) to induce good outcomes. Game-theoretic modeling helps predict the outcome of a given incentive mechanism (in terms of equilibrium) and check whether it is incentive compatible, i.e., users are motivated to act in the intended way [104].

A common game-theoretic model used is the ***Stackelberg game***, which is a leader-follower game. Here, the platform acts as a leader who first announces an incentive scheme (e.g., a reward level or mechanism), and the users are followers who then make their participation decisions. The Stackelberg equilibrium of this game corresponds to an outcome where the leader's strategy is optimal given the followers' best responses, and the followers optimally respond to the leader [105]. Many crowdsourcing incentive problems naturally fit this model: the platform (leader) sets a price or reward, and users (followers) then choose to participate or not based on that reward. At equilibrium, typically, those with cost below a threshold will participate, and the platform's reward is set to balance its need for participants with its budget constraints [94,103]. Each participant i has a cost c_i for performing a task and receives a reward p_i. The agent's utility function is typically given by $u_i = p_i - c_i$, where p_i is determined by the incentive mechanism. A rational participant will only engage in the task if $u_i \geq 0$, leading to the **individual rationality** constraint: $p_i \geq c_i$. If the platform offers a fixed reward R, only participants with $c_i \leq R$ will engage in the task, and the expected participation level is determined by the cumulative distribution function of c_i. Incentive mechanisms are designed to achieve an equilibrium where users have no incentive to deviate from the prescribed strategy. The ***Nash equilibrium*** and *incentive compatibility* conditions in a game with N participants, where each selects s_i, can be unified as:

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \quad \forall s_i \neq s_i^*, \forall i \tag{14}$$

where s_{-i} denotes all other strategies, and s_i^* represents the equilibrium or truthfully reported strategy of user i. This ensures that s_i^* is a stable strategy in equilibrium and that truthful reporting or high effort remains optimal.

4.3.2. Principal-agent theory and mechanism design

The relationship between the crowdsourcing platform (or task requester) and the participants can be viewed through the lens of principal-agent theory. Here, the platform is the principal who wants a task done, and the users are the agents who perform the task. The principal-agent framework is concerned with designing contracts or incentives such that the agents will act in the principal's interest, despite agents having their own interests and typically more information about their own effort or cost (information asymmetry). In crowdsourcing, a key issue is that the platform cannot directly observe a participant's true cost of doing a task or the effort/quality they put in – this is private information of the agent. This leads to classic problems: adverse selection (hidden information, e.g., the platform doesn't know each user's cost or skill level) and moral hazard (hidden action, e.g., the platform cannot perfectly monitor how diligently the user performs the task). Incentive mechanisms are essentially solutions to these problems: they need to encourage truthful revelation of private information (to handle adverse selection) and encourage high effort/performance (to handle moral hazard). Mechanism design is a field of economics (sometimes called reverse game theory) that focuses on designing the rules of a game (mechanism) to achieve a desired outcome. In our context, mechanism design provides methodologies to create payment schemes or scoring rules that lead rational users to behave optimally from the system's perspective. A classic result in mechanism design is the Vickrey-Clarke-Groves (VCG) mechanism for truthful public good allocation; in crowdsourcing, variants of such mechanisms appear in auction-based incentives, where truth-telling is enforced by appropriate reward calculations. For example, paying the second-lowest bid in a reverse auction for sensing tasks ensures truthfulness, as each user's best strategy is to bid their true cost (this aligns with Vickrey auction logic). Many papers formally prove properties like truthfulness, individual rationality, and budget-balance for their proposed mechanisms, which are precisely the concerns of principal-agent theory. Zhang et al. [100] present incentive mechanisms for three crowdsourcing models and prove that each mechanism is individually rational (no participant ends up with negative utility), budget-balanced (the platform doesn't overspend beyond its budget), computationally efficient, and truthful. Ensuring these properties often requires careful payment rules – for instance, giving a bonus equal to the externality a user imposes (VCG logic) or designing a proper scoring rule for submitted data quality. Contract theory, a branch of principal-agent theory, is also applied, especially when dealing with heterogeneous users. The platform (principal) may offer a menu

of contracts – each contract specifying what the user must do (effort, data accuracy, privacy level, etc.) and what reward they get – and each user (agent) will choose the contract that fits their type (cost, ability, or privacy preference). By solving an optimization with incentive compatibility constraints (ensuring each type chooses the intended contract) and participation constraints (each type gets non-negative utility), the platform can derive an optimal set of contracts. A concrete example in crowdsensing is a contract-theoretic incentive mechanism that offers different reward levels for different levels of data privacy the user is willing to forgo [103]. Privacy-conscious users pick a contract with high privacy (and lower reward), whereas others pick lower privacy for higher reward. This screening mechanism ensures each user segment self-selects the contract designed for them, solving the adverse selection. Similarly, one could design contracts for different effort levels or quality levels of contribution. The theoretical frameworks also emphasize equilibrium and optimality concepts like Nash Equilibrium, Stackelberg Equilibrium, and Pareto optimality in the context of incentives. For instance, a well-designed mechanism may achieve a social welfare optimum at equilibrium, meaning the sum of utilities (platform + users) is maximized. Wen et al. [96] claim their quality-driven auction mechanism is social-welfare optimal in addition to being truthful and profitable [103], indicating that at equilibrium the allocation of tasks and payments maximizes total benefit (considering both data quality value and costs). Another design issue is fairness vs. efficiency – sometimes the theoretically optimal (in terms of total output or cost minimization) incentive scheme might not be perceived as fair by participants. For example, an auction that always picks the lowest bidders may over-reward a few and leave others empty-handed frequently, which could hurt long-term participation. Principal-agent theory typically focuses on efficiency and incentive-compatibility, but mechanism designers might introduce fairness constraints or egalitarian considerations as needed [106].

4.3.3. Machine learning (ML) and reinforcement learning (RL) for adaptive incentive optimization

ML techniques have become integral to optimizing incentive mechanisms, enabling platforms to adapt dynamically to complex and uncertain crowdsourcing environments characterized by diverse participant behaviors. ML techniques address critical questions, such as determining optimal reward levels, identifying the most effective incentive types (monetary, gamified, or social), and efficiently allocating limited budgets across tasks to maximize overall outcomes. By utilizing historical data or conducting online experiments, ML algorithms iteratively refine incentive schemes.

RL, in particular, provides a robust theoretical and practical framework for adaptive incentive design. Modeling the incentive allocation process as a Markov Decision Process (MDP), RL allows the platform (agent) to continuously adjust incentives (actions), observe participant responses (reward signals), and optimize strategies over sequential interactions. At each decision point, the platform's choice, such as setting reward levels or selecting incentive structures, influences its current state, including remaining budget or participant engagement levels, and directly impacts immediate and future outcomes. Solving this sequential decision-making problem, RL methods derive policies that maximize cumulative rewards (e.g., task completions, data quality) while minimizing costs. For instance, multi-armed bandit models [107], a specialized RL application, naturally fit incentive optimization scenarios where incentive effectiveness is uncertain. Platforms iteratively explore incentive options (arms), varying rewards or gamification elements, and exploit those showing optimal effectiveness. Truong et al. [108] formalized incentive selection as a multi-armed bandit problem, developing the adaptive HAIS algorithm to dynamically choose incentive schemes and maximize requester utility within budget constraints. Their approach demonstrated empirical effectiveness, achieving 93–98 % of optimal task completion rates and surpassing baseline methods by up to 40 %. ML also supports predictive incentive design through supervised learning methods, such as regression models predicting participant response rates based on offered rewards, timing, and task specifications. Clustering algorithms further enhance personalization by identifying distinct user segments, enabling targeted incentive strategies, for example, distinguishing users more responsive to gamification versus monetary incentives.

Moreover, data-driven mechanism design leverages ML to systematically explore potential mechanism configurations through simulations. Evolutionary algorithms, for instance, iteratively refine auction rules or incentive structures, uncovering effective designs that traditional analytical approaches might overlook. These methods become particularly valuable when addressing complex considerations such as varying user privacy preferences. Wu et al. [103] demonstrated a multi-objective RL approach dynamically adjusting incentive magnitudes while balancing privacy protection, highlighting the versatility of learning-based methods in managing nuanced trade-offs.

A distinctive strength of RL and adaptive mechanism design lies in accommodating user behaviors that deviate from classical rationality assumptions. Unlike traditional game-theoretic models assuming fully rational participants, RL frameworks effectively capture and adapt to real-world behaviors involving biases or bounded rationality. Platforms employing self-play RL can simulate interactions between strategic user models and incentive mechanisms, iteratively refining mechanisms to sustain high engagement even as user responsiveness shifts over time. However, integrating ML-driven adaptability into incentive mechanisms necessitates careful consideration to maintain theoretical properties such as incentive compatibility and fairness. Continuous experimentation inherent to ML methods could inadvertently disadvantage specific user groups if not appropriately managed. Consequently, emerging research emphasizes the convergence of ML methodologies with robust economic theories, termed "mechanism learning", to ensure adaptive mechanisms retain principled economic foundations.

4.3.4. Designing and implementing incentive mechanisms: A step-by-step approach

After reviewing the types, components, technologies, and models of incentive mechanisms, it becomes evident that designing an effective incentive mechanism is a multidisciplinary endeavor that spans from theoretical formulation to practical implementation. A holistic, step-by-step framework is often essential, as ad hoc designs may fail due to unanticipated agent behaviors [109]. To address this complexity, this subsection presents a structured approach for designing incentive mechanisms. Fig. 10 illustrates this process, outlining the core phases involved in systematic incentive design.

1. ***Define Objectives and Desired Outcomes***: Clearly identify what behavior or outcome the mechanism should encourage. Is the goal to increase contributions to a public good, improve data quality, ensure network security, or something else? A precise objective (or multiple objectives ranked by priority) is critical, as it will guide all design choices.
2. ***Model the Environment and Agents***: Develop a model of the participants (agents) and context. Identify who the agents are, what actions they can take, and what their preferences or payoff functions might be. This may involve assumptions about agent rationality, risk aversion, or intrinsic motivations [110]. Modeling also includes understanding the constraints of the environment (budget limits for rewards, technological constraints, etc.).
3. ***Choose the Incentive Structure and Mechanism Type***: Based on the objectives and model, decide what form of incentive to use. Options include monetary incentives (payments, token rewards, profit-sharing), non-monetary extrinsic incentives (points, badges, leaderboards), social incentives (public recognition, reputation points, ranking), and intrinsic boosters (designing tasks to be more inherently enjoyable or meaningful). Often a combination is effective [72].

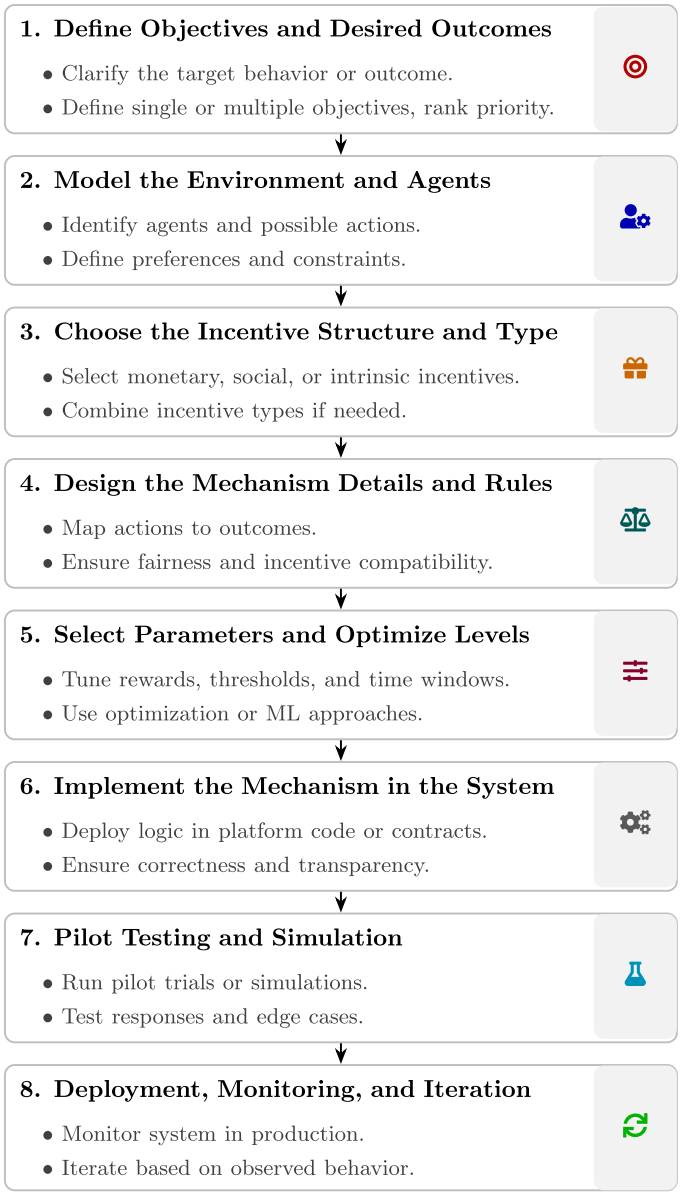

Fig. 10. Step-by-step framework for designing and implementing incentive mechanisms.

4. ***Design the Mechanism Details and Rules***: Specify the exact rules by which incentives will be allocated. This includes the mapping from agent actions or signals to rewards/punishments [70]. If using performance metrics, consider how they could be gamed and add rules to counter that. Using game theory, ensure the mechanism is at least incentive compatible for honest behavior, and revise the rules if it is not.
5. ***Select Parameters and Optimize Incentive Levels***: Most incentive mechanisms involve tunable parameters – the size of rewards or penalties, the threshold to achieve a bonus, the rate of token issuance, the time window for evaluating performance, etc [111]. Optimization techniques (gradient descent, search algorithms, or even machine learning) can be used here to systematically find good parameter sets that achieve the desired trade-offs (e.g., participation vs. cost).
6. ***Implement the Mechanism in the System***: With the design and parameters confirmed, the next step is implementation. This involves programming the rules into the platform or institution where they will operate. For blockchain-based incentives, implementation would be done via smart contracts or protocol code [112].
7. ***Pilot Testing and Simulation***: Before fully rolling out an incentive mechanism, it is wise to test it in a controlled or simulated environment. This could involve running an internal pilot (a subset of users or a simulated set of agents) to observe behaviors.
8. ***Deployment, Monitoring, and Iteration***: Once the incentive mechanism is live, continuous monitoring is required to ensure the mechanism continues to function as expected. If new unwanted behaviors emerge, update the rules to close loopholes. A successful incentive mechanism thus goes through cycles of refinement – design, implement, evaluate, and redesign – much like any engineering system.

Throughout these steps, incentives can change not just behaviors but also values and community atmosphere. Designers should consider whether the mechanism might encourage short-term gains at the expense of long-term motivation (e.g., extrinsic rewards possibly reducing intrinsic interest) and ensure a balance. Mechanism design is often about aligning interests, but when interests cannot be perfectly aligned, transparency and fairness considerations become paramount so that participants accept the system [113].

4.4. Incentive mechanisms and crowd-powered IPS goals

4.4.1. Comparison of incentives in IPS and other crowd-driven domains

This subsection highlights the differences between incentives in IPS and other crowd-driven domains. Unlike other crowd-driven applications, such as traffic monitoring, citizen science, or content annotation, IPS requires users to contribute precise and spatially comprehensive data to ensure accurate positioning services. The incentive mechanisms in IPS must address the unique challenges associated with indoor positioning, including the need for fine-grained localization data, diverse building coverage, and varying user densities. Compared to other crowd-driven applications, IPS faces several distinct challenges that can be summarized as follows:

- *Fine-Grained Localization Data:* Unlike other crowdsourcing tasks that may rely on approximate or generalized data, IPS requires precise positioning information. Accurate sensor readings (e.g., Wi-Fi, BLE, magnetic field, barometric pressure) are highly required to construct fine and reliable indoor fingerprints and models [8,114]. The quality and granularity of these contributions are critical for ensuring the accuracy of location-based services.
- *Building and Floor Diversity with Comprehensive Spatial Coverage:* IPS demands data collection across multiple floors and functionally diverse buildings, each exhibiting different signal propagation characteristics and user densities. Unlike outdoor crowdsourcing, where data is often collected in open spaces, indoor environments present additional complexities due to structural variations. Effective incentive schemes must encourage participation in underrepresented areas, including shopping malls, airports, office buildings, and transit hubs, to prevent spatial gaps in coverage.
- *Temporal and Contextual Consistency for Sustained and Balanced Participation:* Unlike many crowdsourcing applications that can rely on sporadic or one-time contributions, IPS requires continuous data collection across various locations. Indoor environments are dynamic, with frequent changes in signal propagation and infrastructure, necessitating regular updates to maintain database accuracy. Furthermore, incentive mechanisms must ensure balanced participation, preventing an over-concentration of contributions in high-traffic areas while promoting data collection in less-visited locations.
- *Energy and Privacy Constraints:* IPS data collection often involves continuous sensor readings, particularly from power-intensive sources such as Wi-Fi and GNSS, which can significantly impact battery life. Additionally, persistent data collection may raise privacy concerns among users. Effective incentive mechanisms must address these

challenges by optimizing data collection strategies to minimize energy consumption and implementing privacy-preserving techniques that enhance user trust without deterring participation.

By recognizing these distinct challenges, incentive mechanisms for IPS must be carefully designed to align with the system's spatial, temporal, and technical constraints while ensuring sustained user engagement and high-quality contributions.

4.4.2. Objectives of employing incentive mechanisms in crowd-powered IPS

In the previous two subsections, we discussed the general principles behind incentive design and the rationale behind how they can attract user participation. This section focuses on outlining the key objectives the IPS systems aim to achieve through the incentives [115] (i.e., *System Goals*). These goals can be outlined as follows:

- *Localization Reliability-Related Goals:* One of the primary objectives of crowdsourcing in IPS is to ensure reliable annotation and localization of Wi-Fi [8] and magnetic field [116] signatures collected in indoor areas. These signatures often suffer from inaccuracies or high uncertainty due to technological limitations, such as sensor bias and drift [114], as well as human, environmental, and device-related sources of uncertainty. By designing incentives that encourage users to provide precise and verifiable feedback [117], the system can enhance localization reliability. Additionally, it helps validate the reliability of data even in the absence of explicit user feedback, further improving the overall accuracy of the IPS [118].
- *Availability-Related Goals:* Some areas are barely touched by crowdsourcing efforts, leaving data gaps in low-traffic zones [119]. By offering incentives, platforms can motivate users to explore and gather valuable information in these regions, ensuring the system remains widely accessible.
- *Data Quality-Related Goals:* For IPS to be reliable, it needs high-quality data with specific key performance indicators (KPIs). Crowdsourcing can introduce noise or gaps in data quality [120]. Carefully designed incentives can encourage higher-quality submissions, which in turn can help validate or refine lower-quality data, improving overall system robustness [121].
- *Sustainability-Related Goals:* The long-term effectiveness of IPS systems depends on addressing the issue of aging signatures in radio and magnetic maps [122]. These maps can become outdated due to environmental changes [123]. Thus, regular updates are crucial to ensure the system adapts to these changes and maintains its accuracy and reliability.
- *Ubiquity-Related Goals:* Achieving ubiquity in IPS systems means encouraging contributions from diverse users and environments. Effective incentives can drive adoption across different building types, geographic regions, and demographic groups [124]. This inclusive approach ensures a reliable and seamless indoor positioning experience for all users, regardless of location.

By aligning incentive mechanisms with these system goals, IPS can effectively tackle critical challenges such as reliability, availability, sustainability, and ubiquity. Therefore, the strategic design of incentive mechanisms must carefully take into consideration these key objectives.

4.5. Existing incentive mechanisms in crowd-powered IPS

This section reviews the incentive mechanisms developed for crowd-powered IPS, as investigated in the existing literature. A detailed summary of these studies, including their approaches, goals, and effectiveness, is provided in Table 8. To complement this, Fig. 11 visually maps the connections between the mechanisms and their objectives, making their applications and outcomes easier to understand.

4.5.1. The quality-driven auction (QDA) mechanism

The QDA mechanism, introduced by [96], incentivizes workers in MCS systems aiming at prioritizing the quality of submitted data rather than the volume of submissions or time spent working. Unlike traditional methods, QDA emphasizes the utility and reliability of the data. To evaluate data quality, the platform uses utility functions such as $L(x_{ij})$, which measure the value of a specific data point submitted by worker i for task j. This value reflects how well the data aligns with the requester's requirements and supports the platform's objectives. The primary goal of the QDA mechanism is to maximize social welfare by selecting a subset of data submissions that optimizes the following equation:

$$f(W) = \underbrace{R\left(\sum_{W} L(x_{ij})\right)}_{\text{Platform Revenue}} - \underbrace{\sum_{W} k_{ij}}_{\text{Worker Costs}}, \tag{15}$$

where $R(\cdot)$ is the platform's revenue function based on the cumulative quality of the selected data, and k_{ij} is the cost incurred by worker i for task j. This ensures that the system rewards high-quality submissions while minimizing costs, leading to efficient resource utilization. A critical aspect of QDA is platform profitability, which is defined as:

$$u_p = \underbrace{R\left(\sum_{W} L(x_{ij})\right)}_{\text{Platform Revenue from Data}} - \underbrace{\sum_{W} p_{ij}}_{\text{Payments to Workers}}, \tag{16}$$

where p_{ij} is the payment made to worker i for submitting data x_{ij}. The mechanism ensures that the platform's utility remains positive by aligning worker incentives with the platform's objectives. This is achieved by prioritizing data submissions that offer higher reliability and utility.

To maintain fairness and encourage honest participation, QDA incentivizes workers to submit their true costs b_{ij} by making untruthful claims less advantageous. The system leverages a truthfulness property, which guarantees that workers maximize their utility only by reporting their actual costs. The utility for a worker i is defined as:

$$u_i = \sum_{j \in M_i^*} \left[\underbrace{p_{ij}}_{\text{Payment Received}} - \underbrace{k_{ij}}_{\text{Task Cost}} \right], \tag{17}$$

where M_i^* denotes the subset of tasks accepted for worker i. By ensuring $u_i \geq 0$, the mechanism fosters individual rationality, meaning workers are always better off participating than abstaining. QDA's computational efficiency arises from narrowing the search space for winner determination. Instead of evaluating all possible combinations of data submissions, the mechanism prioritizes submissions with higher $L(x_{ij})$ values, significantly reducing computational complexity compared to traditional auction models like reverse Vickrey auctions. In applications such as Wi-Fi fingerprint-based indoor localization, the mechanism evaluates data reliability using models that account for human positioning errors. The reliability of data is factored into $L(x_{ij})$, allowing the system to selectively accept submissions that improve localization accuracy. Despite its strengths, QDA faces challenges such as dependence on worker honesty and the accuracy of the probabilistic models used for quality evaluation.

4.5.2. Spatial coverage expansion (SCE) mechanism

The SCE mechanism [125] addresses the issue of uneven participant distribution in crowdsourcing systems, where contributors cluster in popular areas, leaving less-frequented regions underrepresented. This imbalance hinders tasks such as complete building coverage for 3D modeling or city-wide environmental sensing. The SCE mechanism incentivizes participants to move to less-frequented regions by introducing a movement-based incentive mechanism. A critical feature of the SCE mechanism is its use of a cost function to model the expense incurred by participants for moving to new locations. The moving cost is expressed as:

$$f(d) = e^{\eta d} - 1, \tag{18}$$

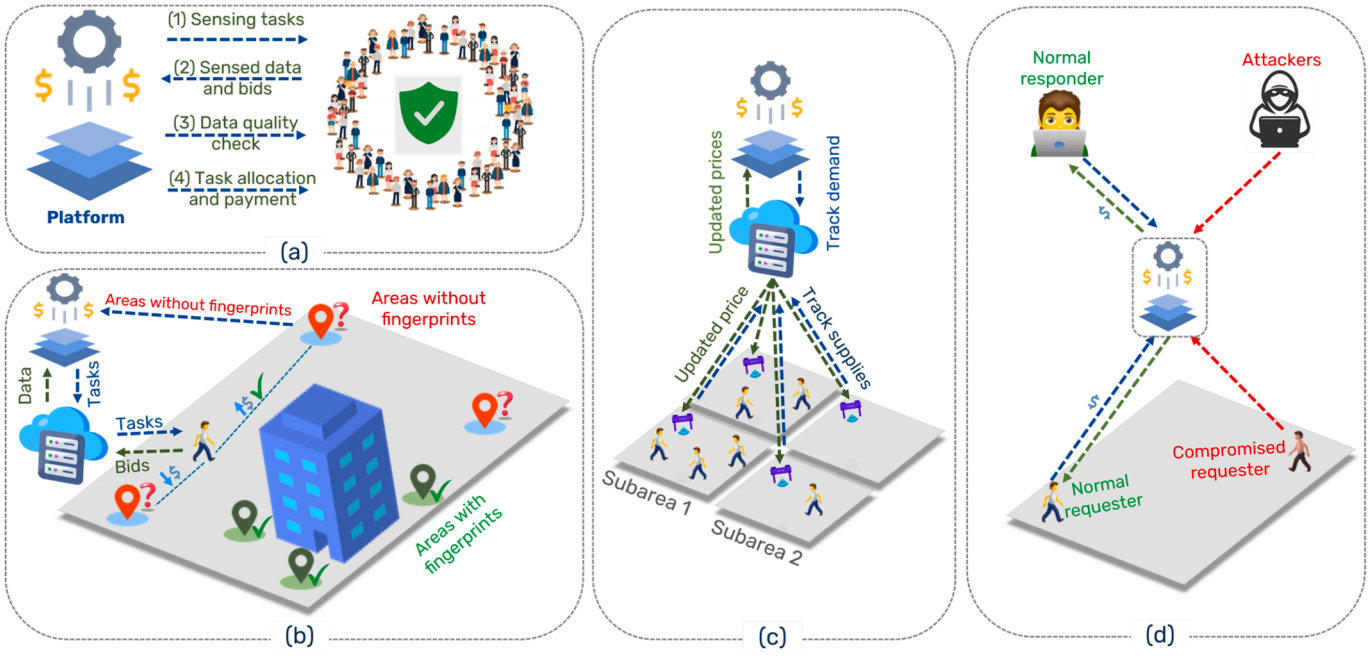

Fig. 11. Incentive mechanisms proposed in the literature: (a) The Quality-Driven Auction (QDA) mechanism, introduced by [96], (figure designed by the authors to visualize the method); (b) The Spatial Coverage Expansion (SCE) mechanism, proposed by [125] to encourage contributors to move to underrepresented areas, (figure created by the authors to better conceptualize and illustrate movement-based incentives); (c) The Equilibrium-Driven Incentive (EI) mechanism, proposed by [126], (figure inspired by [126] and redesigned by the authors with 3D plotting for improved clarity); and (d) The Responders' Behaviors-Based Reputation (RBR) mechanism, developed by [127] to reward responders based on their behavioral patterns, (figure designed by the authors to illustrate the method).

where d is the distance moved, and η is a scale factor reflecting environmental and individual factors such as time and energy. The mechanism employs a reverse auction framework, where participants submit bids that include their movement costs. The platform allocates tasks and payments using a greedy algorithm to maximize social welfare. The social welfare function is defined as:

$$w = \sum_{i \in N} \left[\underbrace{\sum_{t \in S_i} (v_t - c_i)}_{\text{Task Value for Participant } i} - \underbrace{f_{\eta_i}(d_i)}_{\text{Moving Cost for } i} \right], \tag{19}$$

where v_t is the value of task t, c_i is the cost for participant i to complete a task, and $f_{\eta_i}(d_i)$ is the moving cost for participant i. Since the task allocation problem is NP-hard, the SCE mechanism employs a greedy algorithm that iteratively selects participants who maximize their contribution to social welfare:

$$\arg\max_i \left[\sum_{t \in S_i} (v_t - c_i) - f_{\eta_i}(d_i) \right]. \tag{20}$$

To ensure truthful cost declarations, the SCE mechanism incorporates a critical payment policy. The payment to a participant i is determined as:

$$p_i = |S_i| \cdot c_i + f_{\eta_i}(d_i), \tag{21}$$

where $|S_i|$ is the number of tasks completed by participant i. This guarantees that participants have no incentive to misreport their costs, fulfilling the truthfulness property. The SCE mechanism achieves several desirable properties: 1) Truthfulness: Participants are incentivized to declare their true costs; 2) Individual Rationality: Ensures that the payoff for each participant is non-negative; 3) Platform Profitability: Guarantees the platform's utility remains positive; and 4) Computational Efficiency: The greedy algorithm ensures the solution is computationally feasible. The mechanism has been validated through simulations, showing significant improvements in task completion ratios and social welfare compared to traditional methods like MSensing. For instance, when participants are clustered in popular areas, SCE effectively motivates movement to unpopular areas, achieving up to a 145 % increase in task completion under certain scenarios. Despite its advantages, SCE faces challenges such as dependency on accurate cost modeling.

4.5.3. Equilibrium-driven incentive (EI) mechanism

EI mechanism [126] balances the supply and demand for fingerprint data in mobile crowdsourcing systems, optimizing benefits for all stakeholders, including the crowdsourcer, mobile users, and the overall system. The mechanism relies on the Walrasian equilibrium model to eliminate monopolistic control and ensure fair pricing and efficient resource allocation, as illustrated in Fig. 11(c). In this mechanism, the target area is divided into multiple subareas, each with adaptive demand set by the crowdsourcer. Mobile users contribute Channel State Information (CSI) fingerprints, and their contributions are measured based on trajectory distance. The social welfare of the system is defined as:

$$J = \underbrace{\sigma \prod_{j=1}^{N} D_j^{w_j}}_{\text{Crowdsourcer Utility}} - \underbrace{\sum_{k=1}^{M} \left(a_k d_k^2 + b_k d_k \right)}_{\text{Mobile Users' Costs}}, \tag{22}$$

where D_j is the total trajectory distance demanded in subarea j, a_k and b_k are cost coefficients for user k, and σ and w_j are elasticity coefficients reflecting the crowdsourcer's preference for higher-quality data. The utility of the crowdsourcer is expressed as:

$$W = \underbrace{\sigma \prod_{j=1}^{N} D_j^{w_j}}_{\text{Payoff from Data}} - \underbrace{\sum_{j=1}^{N} p_j D_j}_{\text{Payments to Mobile Users}}, \tag{23}$$

where p_j is the price per unit of trajectory distance in subarea j. Mobile users aim to maximize their utility while minimizing costs. The utility function for a mobile user k in subarea j is:

$$V_k = \underbrace{p_j d_k}_{\text{Earnings from Contribution}} - \underbrace{\left(a_k d_k^2 + b_k d_k \right)}_{\text{User's Costs}}, \tag{24}$$

where d_k is the trajectory distance contributed by user k. The coefficients a_k and b_k reflect individual differences in time and resource availability. The Walrasian equilibrium ensures that demand matches supply in each subarea:

$$D_j = \sum_{k \in A_j} d_k, \tag{25}$$

where D_j is the total demand in subarea j, and $\sum_{k \in A_j} d_k$ represents the total supply from users in that subarea. This condition guarantees market clearing, achieving a Pareto optimal state where all stakeholders' utilities are maximized. To achieve equilibrium, the system employs an iterative price adjustment process. At each iteration, the prices are updated as:

$$\lambda_j^{r+1} = \lambda_j^r + \alpha\Big(D_j^r - \sum_{k \in A_j} d_k^r\Big), \tag{26}$$

where λ_j is the price for subarea j at iteration r, and α is the step size controlling the convergence speed. The EI mechanism has been validated through simulations, demonstrating its ability to converge to optimal solutions while achieving high social welfare. The results show improved fairness and efficiency compared to traditional crowdsourcer-centric schemes, highlighting the potential of Walrasian equilibrium in incentivizing fingerprint data collection for indoor localization.

4.5.4. Responders' behaviors-based reputation (RBR)

The RBR mechanism [127] is designed to incentivize positive behaviors in a crowdsourcing-based indoor navigation system (CINS), as shown in Fig. 11(d). It employs an offensive-defensive game model and replicator dynamics to address challenges such as collusion between responders and requesters, which can undermine the credibility of the reputation system. The mechanism ensures fair task allocation and maximizes social welfare while maintaining system security. In this mechanism, requesters initiate tasks via a fog server platform, which selects responders based on their reputation. After completing the task, requesters evaluate the quality of service provided by responders, updating their reputation. Responders are rewarded based on the fees paid by requesters, where a portion $\delta\%$ of the fee is allocated to responders, and the remaining $1-\delta\%$ goes to the platform. The reputation value R for responders and the platform is updated dynamically based on task outcomes and interactions. The system uses an offensive-defensive game to model interactions between the fog server platform and responders. Responders can adopt one of two strategies: positive service or collusion. Collusion increases the attacker's utility but risks detection and penalties. The degree of collusion is quantified as:

$$\lambda = \frac{1}{1 + e^{-[f(i,j)g(C_u, N_u)]}}, \tag{27}$$

where $f(i,j)$ represents the social relationship between requesters and responders, and $g(C_u, N_u)$ is a function of the number of attacks C_u and compromised requesters N_u. Responders' utility is influenced by their reputation and the quality of service they provide. A responder's utility when adopting collusion is:

$$U_a = \sum_{k=1}^{k_d} \Bigg[\underbrace{\delta\alpha_k}_{\text{task income}} - \underbrace{\lambda\beta c_1}_{\text{collusion cost}} - \underbrace{P\xi\lambda}_{\text{detected penalty}} + \underbrace{(1-P)\rho\lambda}_{\text{undetected reward}} \Bigg] + \underbrace{\delta e^{\phi(1-\lambda)}(B_{i\to p} + \gamma N_{i\to p})}_{\text{future utility}}, \tag{28}$$

where α_k is the income from task k, β represents the quality of the navigation path, c_1 is the cost of collusion, and P is the probability of being detected. The platform's utility is derived from successful supervision, cost minimization, and reputation preservation. Its utility is expressed as:

$$U_d = \sum_{k=1}^{k_d} \Bigg[\underbrace{(1-\delta)\alpha_k}_{\text{platform revenue}} - \underbrace{d_1}_{\text{supervision cost}} + \underbrace{P\eta\lambda}_{\text{supervision reward}} - \underbrace{(1-P)\sigma\lambda}_{\text{collusion penalty}} \Bigg] + \underbrace{(1-\delta)e^{\phi(1-\lambda)}(B_{i\to p} + \gamma N_{i\to p})}_{\text{future utility}}, \tag{29}$$

where d_1 is the cost of supervision, and σ is the loss due to successful collusion. To stabilize the system, replicator dynamics are used to adjust strategies dynamically. The growth rate of a strategy is proportional to the difference between its utility and the average utility. This is expressed as:

$$\frac{dx}{dt} = x\big[U_a - \bar{U}_a\big], \quad \frac{dy}{dt} = y\big[U_d - \bar{U}_d\big], \tag{30}$$

where x and y are the probabilities of responders colluding and the platform supervising, respectively. The RBR mechanism enhances system security by integrating supervision and dynamic reputation updates. Simulations show that the mechanism effectively reduces collusion and increases social welfare compared to traditional models. However, the mechanism's effectiveness depends on the accuracy of reputation evaluation and the computational efficiency of the game-theoretical model.

4.5.5. Differential privacy-enabled (DPE) mechanism

The DPE mechanism [128] is designed to incentivize mobile users (MUs) to contribute trajectory data for crowdsourcing-based indoor localization while preserving their privacy. It employs two reward mechanisms tailored to different privacy information scenarios. The first mechanism addresses incomplete information about MUs' privacy sensitivity and uses a fixed reward, while the second mechanism assumes complete information and offers variable rewards to optimize participation. The first mechanism formulates the interaction between the crowdsourcing platform (CP) and MUs as a two-stage Stackelberg game. In this game, the CP acts as the leader, announcing a fixed reward R to attract MUs. MUs then respond by deciding their participation strategy to maximize their utility. The trajectory utility of an MU i is defined as:

$$g(d_i, \epsilon_i) = \Big[\pi_1 - \pi_2 e^{\pi_3(1-\epsilon_i)}\Big] d_i, \tag{31}$$

where d_i is the trajectory length, ϵ_i is the privacy budget, and π_1, π_2, π_3 are system parameters ensuring positivity and diminishing utility with stronger privacy guarantees. The utility function of an MU combines trajectory utility and the cost of privacy loss:

$$U_i = \underbrace{\frac{g(d_i, \epsilon_i)}{\sum_{j \in N} g(d_j, \epsilon_j)} R}_{\text{Reward Component}} - \underbrace{\epsilon_i \tau_i d_i}_{\text{Privacy Cost Component}}, \tag{32}$$

where τ_i represents the MU's unit cost for privacy loss, and N is the set of participating users. This formulation ensures that MUs balance privacy concerns with rewards when deciding their participation. The CP maximizes its profit while ensuring privacy protection. The profit function for the CP is defined as:

$$U_{\text{CP}} = \underbrace{\chi \log\Big(1 + \sum_{j \in N} \log(1 + d_j)\Big)}_{\text{Data Contribution Revenue}} - \underbrace{R}_{\text{Total Reward Paid}}, \tag{33}$$

where χ is a parameter representing the CP's preference for higher-quality data, and the logarithmic terms account for diminishing returns

on trajectory length and number of participants. The second mechanism introduces variable rewards and assumes that the CP has complete information about MUs' privacy sensitivities. A demand function models the relationship between the CP, MUs, and service customers (SCs):

$$Q = \underbrace{Q_0}_{\text{Base Demand}} + \underbrace{\alpha p}_{\text{Positive Externality}} - \underbrace{\beta q}_{\text{Price Sensitivity}}, \tag{34}$$

where Q is the service demand, Q_0 is the base demand, αp represents the positive externality of higher data-buying prices p, and β is the sensitivity of SCs to higher service prices q. The CP's profit under the variable reward mechanism is expressed as:

$$U_{\text{CP}} = \underbrace{Qq\delta \log\left(1 + \sum_{i \in S} \log(1 + d_i)\right)}_{\text{Service Revenue}} - \underbrace{\sum_{i \in S} p}_{\text{Payment to MUs}}, \tag{35}$$

where δ reflects the CP's preference for higher-quality data, and S is the set of MUs with non-negative utility. Simulations demonstrate that the DPE mechanism effectively balances privacy protection and participation incentives. The fixed reward mechanism provides robust privacy guarantees under incomplete information, while the variable reward mechanism achieves higher profits by leveraging complete privacy information. Both mechanisms highlight the importance of tailored incentives in enhancing the effectiveness of crowdsourcing-based indoor localization systems.

4.6. Quantitative evaluation and gaps of existing incentive mechanisms in crowd-powered IPS

4.6.1. Quantitative evaluation of existing incentive mechanisms in crowd-powered IPS

This section provides a comprehensive quantitative analysis of existing incentive mechanisms used in crowd-powered IPS. The evaluation benchmarks performance across various criteria, including social welfare, task completion ratio, platform profitability, participant truthfulness, and computational efficiency. Table 7 summarizes these quantitative findings from the literature, offering a comparative overview that highlights each mechanism's strengths and limitations. Key evaluation metrics include:

- Social Welfare: Measures the overall effectiveness and resource optimization of the incentive mechanism.
- Task Completion Ratio: Represents the proportion of successfully completed tasks.
- Platform Profitability: Indicates the economic sustainability of the crowdsourcing platform.
- Truthfulness: Evaluates whether the incentive mechanism motivates honest behavior among participants.
- Computational Efficiency: Reflects the practical applicability, measured in terms of complexity or convergence speed.

QDA Mechanism achieves high social welfare and robust profitability through quality-driven incentives but depends significantly on accurate data quality assessment and truthful bidding mechanisms. SCE Mechanism excels in improving task completion rates, especially when motivating users to cover spatially unpopular regions, strongly outperforming traditional fixed-location schemes. EI Mechanism demonstrates superior performance by achieving Pareto optimality, benefiting all parties involved (platform, users, and system), while quickly converging to equilibrium. RBR Mechanism provides strong social welfare improvements through its effectiveness at reducing collusion, though computationally more demanding due to dynamic reputation updates and com-

Table 7
Quantitative evaluation of existing incentive mechanisms for crowd-powered IPS.

Mechanism	Social Welfare	Task Completion Ratio	Platform Profitability	Truthfulness	Computational Efficiency
Quality-Driven Auction (QDA) [96]	High (150 % increase compared to Vickrey auctions)	High (>70 %)	Positive profitability guaranteed	Yes (fully truthful)	High (polynomial complexity $O(n^2 m \log m)$)
Spatial Coverage Expansion (SCE) [125]	High (significantly better than MSensing)	High (up to 70 %, improves significantly with increased mobility incentives)	Positive (profits grow with more spatial coverage)	Yes (fully truthful through critical payments)	High (polynomial complexity with greedy algorithm $O(n^2 m \log m)$)
Equilibrium-Driven Incentive (EI) [126]	Very High (Pareto optimal)	Balanced (supply-demand equilibrium guarantees task completion)	High (optimal pricing balance ensures positive profit)	Implicitly truthful (Walrasian equilibrium)	High (fast convergence through iterative dual decomposition, convergence within 50–100 iterations)
Responders' Behaviors-Based Reputation (RBR) [127]	High (enhanced by reduced collusion)	Moderate to High (improves significantly with effective reputation dynamics)	High (platform profits significantly from effective supervision)	Partial (relies on dynamic reputation)	Moderate (complexity introduced by replicator dynamics and offensive-defensive game, but converges to stable equilibrium)

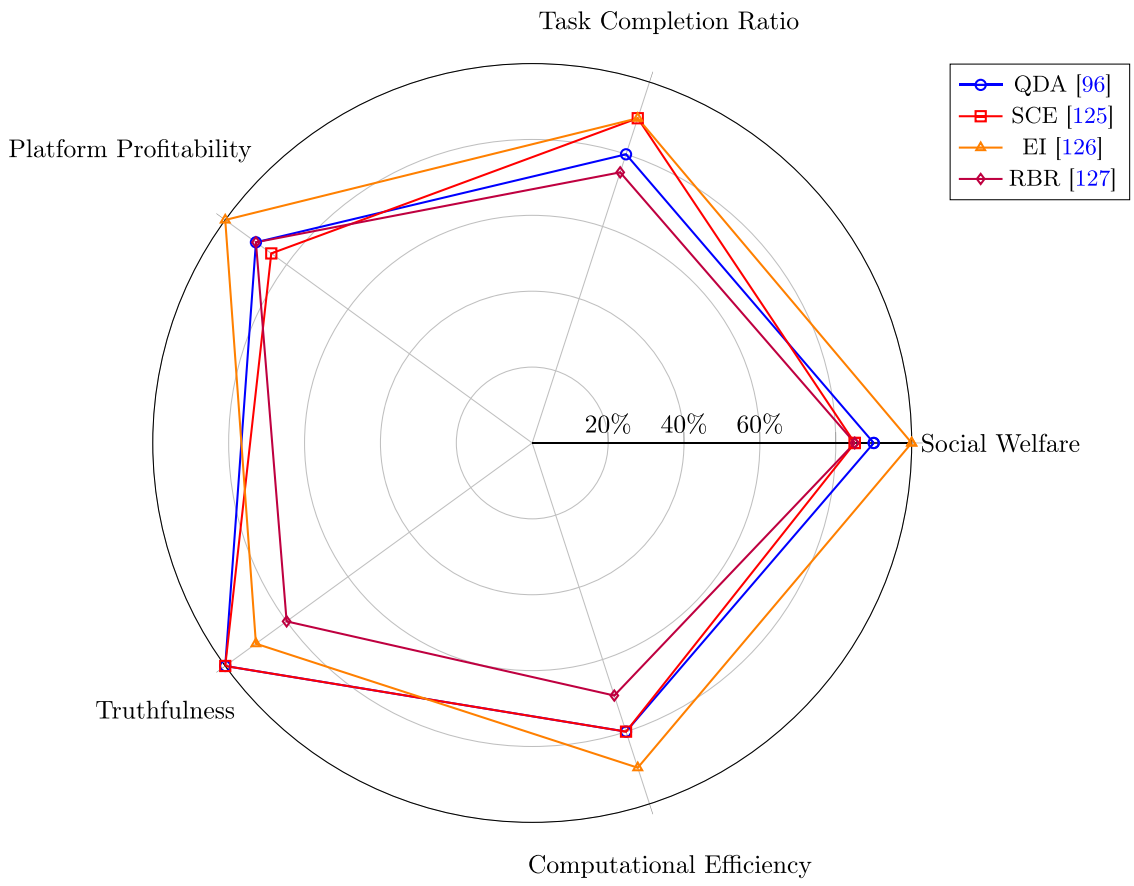

Fig. 12. Comparative performance of existing incentive mechanisms proposed in existing crowd-powered IPS.

plex game dynamics. Fig. 12 presents a radar chart illustrating the comparative performance of the four incentive mechanisms (QDA, SCE, EI, RBR) across key evaluation metrics.

4.6.2. Gaps in existing incentive mechanisms

Despite the advantages offered by existing incentive mechanisms in crowd-powered IPS, several challenges persist in their design and implementation. This section explores the key gaps and limitations in these mechanisms. One significant gap lies in the misalignment between the proposed incentives and the objectives they aim to achieve in many existing studies. This disconnect can lead to increased system costs and hinder scalability. However, this issue could be mitigated by tailoring incentive types to align more closely with system goals. For instance, the QDA mechanism [96] effectively encourages high-quality data submissions but relies heavily on the availability of accurate data quality metrics. Unfortunately, these metrics are not clearly defined in the study, despite being central to the mechanism's success. Additionally, QDA could integrate incentive motivations with rewards to reduce costs further. Similarly, the SCE mechanism [125] enhances spatial coverage in less-visited areas but depends on precise cost modeling. Its greedy algorithm, while effective, may not always produce globally optimal solutions. SCE could also leverage users' willingness to explore new areas or exercise more frequently by incorporating gamified incentives, reducing costs while catering to diverse user motivations. The EI mechanism [126] demonstrates success in balancing supply and demand but is highly sensitive to variations in demand reports. Achieving equilibrium often requires iterative price adjustments, which may complicate its implementation. Mechanisms like RBR [127] ensure fairness and discourage collusion but are susceptible to reputation manipulation. They require robust supervisory systems to prevent misuse effectively. Finally, the DPE mechanism [128] strikes a balance between privacy protection and data contribution. However, it may compromise accuracy to maintain privacy and is highly sensitive to the settings of its privacy budget, which poses challenges for widespread adoption.

4.7. Concluding remarks

In summary, incentive mechanisms in crowd-powered IPS are central to sustaining participation, ensuring data quality, and achieving comprehensive spatial and temporal coverage. The review of monetary, non-monetary, and hybrid models, alongside their underlying theoretical and technological foundations, highlights the diversity of approaches available and their varied alignment with IPS-specific objectives. Comparative analysis of existing mechanisms underscores that no single strategy fully addresses all IPS challenges, reinforcing the need for context-aware, goal-oriented, and adaptable incentive designs. This understanding provides a clear foundation for the subsequent section on privacy and security considerations, where the balance between motivation and user trust becomes critical.

5. Privacy and security in crowd-powered IPS

This section begins by outlining the risks and protection requirements across the MCS lifecycle, setting the foundational context for subsequent discussions. It then summarizes key privacy and security techniques developed for general MCS applications. Building on this, the section reviews existing privacy-preserving mechanisms specifically tailored to crowd-powered IPS, followed by a discussion of complementary security-preserving strategies. Finally, it identifies critical gaps and limitations in current solutions.

Table 8
Gaps and limitations in existing incentive mechanisms for crowd-powered IPS.

Mechanism	Key Gaps and Limitations	Potential Mitigations
Quality-Driven Auction (QDA) [96]	Relies heavily on accurate data quality metrics, which are not well-defined. This increases system costs and reduces scalability.	Define clear and reliable data quality metrics. Integrate incentive motivations, such as rewards and gamification, to reduce costs further.
Spatial Coverage Expansion (SCE) [125]	Depends on precise cost modeling, which may not always reflect user behavior. The greedy algorithm may fail to achieve globally optimal solutions.	Incorporate gamified incentives to encourage users to explore new areas or exercise. Use advanced optimization algorithms for global solutions.
Equilibrium-Driven Incentive (EI) [126]	Highly sensitive to variations in demand reports. Achieving equilibrium often requires iterative price adjustments, complicating implementation.	Develop robust demand estimation techniques to reduce sensitivity. Simplify price adjustment methods for practical implementation.
Responders' Behaviors Reputation (RBR) [127]	Susceptible to reputation manipulation and requires robust supervisory systems to prevent misuse.	Implement tamper-proof reputation systems, such as blockchain or distributed ledger technologies. Strengthen supervisory frameworks.
Differential Privacy-Enabled (DPE) [128]	May compromise accuracy to maintain privacy. Highly sensitive to privacy budget settings, challenging widespread adoption.	Optimize privacy budget settings to balance privacy and accuracy. Provide user education on the benefits of privacy-preserving mechanisms.

5.1. Overview of privacy and security risks and protection strategies across the MCS lifecycle

5.1.1. Overview of privacy and security risks

The data linked to user location serves as a mirror reflecting user behavior and preferences [129]. While this data is beneficial for advertising and recommendation systems, it also contains sensitive information and poses significant risks if exposed to hacking. Malicious actors represent a serious threat, as they can analyze Wi-Fi signals and monitor patterns to infer a client's daily routines and activities [130], thereby endangering participant safety [131]. In crowdsourcing, localization data is typically collected and analyzed in the cloud, with results transmitted back to users to improve real-time positioning [132]. Consequently, these systems remain highly vulnerable to malicious attacks, which may be motivated by:

- Manipulating data for personal gain or competitive advantage.
- Violating user privacy through unauthorized access to sensitive information.
- Disrupting system functionality to cause inconvenience or financial losses.
- Exploiting resources without authorization.

Accordingly, numerous studies have addressed the security and privacy of crowd-powered IPS to mitigate the risks of such attacks and to improve user willingness to participate.

5.1.2. Privacy protection strategies across the MCS lifecycle

Privacy protection is critical at every stage of the MCS lifecycle due to the sensitivity of user-contributed data and the diverse vulnerabilities present during system operation. Table 9 offers a structured classification of key privacy risks, corresponding defense strategies, technical methods, and implementation challenges encountered at each phase of the MCS process.

Initially, the *task design and allocation* phase involves defining crowdsensing tasks, which inherently carry risks related to user consent, sensitivity of the requested data, and identity leakage during task dissemination. To counteract these risks, strategies such as location obfuscation based on local differential privacy (LDP), encrypted task descriptors, and anonymous bidding protocols are commonly employed. For instance, local DP schemes have been utilized for routing tasks anonymously, while encrypted descriptors safeguard task content from unauthorized exposure [133,134]. Nevertheless, deploying these solutions faces notable challenges, especially the absence of widely usable and intuitively designed user interfaces that reliably preserve user anonymity and encourage broad participation [135].

During the *user recruitment and incentive* phase, privacy threats shift toward identity inference via incentive structures and reward-tracking mechanisms. Effective countermeasures include privacy-preserving incentive frameworks that leverage anonymous credential systems, DP-based privacy auctions, and blockchain-based platforms that facilitate verifiable yet anonymous rewards. DP mechanisms establish a rigorous privacy framework for user bids, complemented by blockchain-enabled smart contracts that offer transparent yet secure rewards [136]. However, notable implementation challenges remain, particularly navigating the trade-off between transparency and anonymity and enhancing resistance to collusion attacks within incentive schemes.

The subsequent phase of *data collection* is particularly vulnerable to location disclosure, identity re-identification, and the inadvertent capture of sensitive contextual information. To protect users' privacy at this critical juncture, advanced methods such as federated learning (FL), LDP noise injection, blockchain-secured data traces, and homomorphic encryption (HE) have been widely adopted. Implementations such as the CrowdFL framework integrate FL to keep raw data localized on user devices while aggregating only model updates centrally [138]. Additionally, local DP perturbation and HE schemes (e.g., Paillier encryption) provide formal confidentiality guarantees prior to any centralized computation [133,139]. Despite their effectiveness, these techniques often impose considerable energy and computational demands on user devices, posing a key challenge to real-world scalability [140].

Once collected, data moves into the *aggregation and analysis* phase, where it faces threats from unauthorized disclosures, compromise of secure aggregation protocols, and statistical inference from collective patterns. Consequently, techniques such as secure multi-party computation (SMPC), HE-based aggregation, and DP-guided data fusion have been introduced to address these vulnerabilities. Notable examples include the BLIND system, which uses SMPC and encryption to secure computations, and the Multi-Functional Homomorphic Encryption (MFHE) approach, both enabling collaborative analysis without revealing individual data [139,141,142]. However, these advanced solutions encounter significant barriers, including elevated computational demands, complex inter-party synchronization, and scalability limitations, reducing their feasibility in large-scale real-world deployments [143].

During the crucial *truth discovery* phase, the accuracy and integrity of aggregated data are at risk from malicious input manipulation, poisoning attacks, and adversarial interference. To support trustworthy and privacy-preserving truth inference, techniques such as DP-enhanced robustness, encrypted reputation models, zero-knowledge proof (zk-proof) verification, and reputation-aware federated learning have been deployed. For example, the BLIND system's encrypted reputation mechanism exhibits resilience to data manipulation, while zk-proof protocols and blockchain-backed trusted execution environments (TEEs) reinforce the validity of derived truths [141,144,145]. Still, scalability and validation of these advanced solutions remain challenging due to their computational intensity and architectural complexity.

Table 9
Classification of privacy threats and protection strategies across MCS phases.

MCS Phase	Privacy Threats	Privacy Protection Strategies and Technical Details	Implementation Examples and Challenges
Task Design & Allocation	Consent, task sensitivity, identity leakage	Location-obfuscation, encrypted task allocation, and anonymous task bidding. Uses local differential privacy (LDP) and secure encrypted descriptors for consent-preserving task dissemination.	**Examples:** Local DP schemes for task routing [133]; encrypted descriptors in [134]. **Challenges:** Lack of practical user platforms [135].
User Recruitment & Incentive	Incentive inference, identity traceability, recruitment privacy, incentive leakage	Privacy-preserving incentive models via anonymous credentials (e.g., blind signatures), DP-based bidding, and blockchain auctions with verifiable rewards.	**Examples:** DP-based incentives [136]; smart contract reward flows [137]. **Challenges:** Balancing fairness and anonymity; collusion resistance.
Data Collection	Re-identification, location leakage, unintended sensing of personal info	Techniques include federated learning (FL), homomorphic encryption (HE), blockchain logging, and local DP (LDP). Protects raw data on device before upload.	**Examples:** CrowdFL framework [138]; local DP in [133]; HE in [139]. **Challenges:** Resource constraints noted in [140].
Data Aggregation & Analysis	Secure aggregation, inference from data patterns, access misuse	Secure multi-party computation (SMPC), HE-based aggregation (e.g., Paillier), and differential privacy-aware fusion. Two-party computing or encrypted summation used in frameworks like BLIND and MFHE.	**Examples:** BLIND [141]; MFHE approach [142]; encrypted summation [139]. **Challenges:** Coordination and computational overhead [143].
Truth Discovery	Input tampering, data poisoning, integrity attacks	Resilient truth estimation using DP and encrypted aggregation under adversarial conditions. Techniques include poisoning detection, zk-proofs, and reputation-weighted FL.	**Examples:** Encrypted reputation in BLIND [141]; adversary resilience in [144]; integrity via TEE-Blockchain [145]. **Challenges:** High validation complexity; scalability.
Data Feedback & Trading	Transaction traceability, feedback linking to identity	Mix networks, blind token schemes, and pseudonymous reward systems for protecting feedback-related identity leakage. Blockchain ensures auditability.	**Examples:** PARS token design [146]; CrowdBLPS for location-trace unlinkability [147]. **Challenges:** Feedback privacy and unlinkability trade-offs [140].
Reward & Recognition	Re-identification from scores or public acknowledgements	Zero-knowledge proof (ZKP)-based reward claims, anonymous leaderboard mechanisms, and score verification without linking to personal IDs.	**Examples:** private redemption in [146]; privacy-preservation with efficient reputation management [36,37]. **Challenges:** Sparse adoption; system design complexity [148].

At the *data feedback and trading* stage, concerns regarding transaction traceability and the linkage of user identities through feedback mechanisms arise. To address these privacy threats, technologies such as blind signatures, anonymous reward tokens, and pseudonymous marketplace interactions have been proposed and deployed. Systems like PARS, utilizing blind token schemes, and CrowdBLPS, which integrates blockchain-based mechanisms to maintain transaction unlinkability, provide effective practical examples of these approaches [146,147]. However, finding an optimal balance between maintaining user anonymity and ensuring accountability and transparency within such feedback and trading mechanisms continues to pose unresolved research challenges [140].

Finally, in the *reward and recognition* phase, privacy concerns predominantly revolve around user re-identification from published scores, rewards, or public acknowledgments. Privacy-preserving measures have been implemented to mitigate these threats, including zero-knowledge proof-based reward claims, anonymous leaderboards, and unlinkable reputation management systems. For example, [36,37] propose a lightweight privacy-preservation approach coupled with efficient reputation management. Anonymous scoring and private redemption schemes effectively protect participant identities while still enabling fair reward recognition [146]. Nevertheless, their limited adoption and considerable system design complexity remain critical barriers that need further exploration and practical resolution [148].

5.2. Key techniques for privacy and security protection in general MCS applications

MCS systems face critical privacy and security challenges due to the sensitive nature of user-contributed data and the need for trustworthy aggregation. A variety of protection methods have been developed to safeguard participants' information while still enabling useful data analysis. This subsection surveys these protection strategies, highlighting their implementation in MCS applications and integration into recent research work.

5.2.1. Anonymization and pseudonymity in MCS

Anonymization techniques in MCS aim to dissociate user identities from their contributed data. Instead of attaching a static user ID to each

submitted data point, systems often use pseudonyms or one-time identifiers that prevent direct identification of the source [149]. For example, Tang et al. [144] design an anonymization protocol (AnonymTD) that assigns each participant a random sequence number for each task, so that the server can obtain the data without knowing which worker sent it. By using such transient pseudonyms, multiple submissions from the same user cannot be linked, greatly reducing the risk of profiling a user's behavior. Other frameworks leverage trusted intermediaries or cryptographic mix networks: a trusted server (or a set of servers) can strip identifying information or shuffle data submissions before they reach the aggregator, ensuring that the mapping from users to data is hidden. For instance, a privacy-aware credentialing approach can issue anonymous tokens or certificates to users, which are used to authenticate data uploads without revealing the user's true identity. This idea is realized in systems where mobile clients authenticate via group signatures or attribute-based signatures, obtaining signed tokens that allow data submission under a pseudonym that the platform cannot trace back to the real identity [140]. These pseudonym schemes often include provisions for strong unlinkability (the platform cannot link different contributions to the same user) and conditional privacy, meaning that a misbehaving user can be identified only by a trusted authority if absolutely necessary (e.g., in case of abuse).

5.2.2. Data perturbation and obfuscation

Data perturbation is a straightforward yet effective privacy technique in which each user adds noise to or perturbs their data before sharing it. The goal is to obfuscate sensitive exact values while still allowing useful aggregate information to be extracted. In MCS, this can take many forms: users might add random noise to sensor readings, report a slightly blurred location instead of their precise coordinates, or quantize data to a coarse level. For example, a participant reporting their location could snap it to a nearby grid intersection or add a random offset of a few tens of meters, so that the exact position is hidden. This protects privacy at the cost of some accuracy. Perturbation can be as simple as adding noise drawn from a certain distribution to each data point. If the noise is zero-mean and independent, the aggregate (e.g., the average of many users' readings) can still converge to the true value as more data are collected, while any single user's contribution is masked.

A concrete implementation of perturbation in MCS is given by Tang et al. [144] in their PerturbTD protocol. In scenarios where users are even willing to share an estimate of their reliability weights, they avoid heavy cryptography by using random perturbation. Each worker perturbs their data readings with some randomness before uploading. The system then utilizes two non-colluding cloud servers to process these perturbed values. Essentially, the noise added by users can be canceled out by appropriate cooperation between the servers: one server might get an aggregate of "data + noise" and the other aggregates the "noise" contributions, so that by exchanging partial results the true aggregate can be obtained without either server seeing any user's raw data. This two-server architecture (a common variant of secure multi-party computation) allows most of the heavy truth discovery computation to be done on the server side while keeping each individual's data private. The trade-off here is that if the two servers were ever to collude, privacy would break; but by assuming they are run by independent organizations, users' privacy is preserved with much lower overhead than fully homomorphic encryption.

More generally, data perturbation techniques impose minimal computational cost on users, since adding random noise or performing a simple data transformation is lightweight. This makes perturbation attractive for battery-limited smartphones. However, perturbation inevitably introduces errors. The magnitude of noise must be carefully calibrated: too little noise may fail to protect privacy, whereas too much noise can destroy the utility of the crowdsensed data.

5.2.3. Differential privacy for crowdsensed data

DP is a strong mathematical privacy standard that has been increasingly applied to crowdsensing data. At a high level, DP ensures that the inclusion or exclusion of any single participant's data does not significantly affect the outcome of a query or analysis, thereby limiting what an adversary can learn about that individual [150]. In an MCS context, this typically means algorithms are designed so that the final reported statistics (e.g., aggregated results) have a carefully injected noise component. Formally, a mechanism is ϵ-differentially private if changing one user's data (while keeping others' the same) changes the probability of any given output by at most a factor e^{ϵ} [151]. A smaller ϵ implies stronger privacy (and more noise added).

There are two main ways DP is employed in MCS: central DP and local DP. In central (or global) DP, the aggregator (server) collects exact data from users, then adds noise to the results or queries it publishes. This requires users to trust the server with raw data (which might be unacceptable if the server itself could be compromised). In contrast, LDP has each user randomize their data before sending it, so even the server never sees the true values. LDP is stronger in the trust model (no trusted server needed), but typically requires injecting more noise to achieve the same accuracy because the randomization happens at the individual level. Research in MCS leans towards LDP methods, to avoid reliance on a trusted central party [152]. For instance, Cui et al. [133] develop a crowdsensing data aggregation scheme based on LDP, where each user's phone adds calibrated Laplace noise to sensor readings according to a privacy budget, and the server statistically estimates the true aggregate from the noisy reports.

One challenge specific to crowdsensing is that data from one user may arrive as a time series or correlated set, violating the usual assumption of independent contributions. Chen et al. [153] highlight that applying vanilla differential privacy independently to each data point can leak more information than expected if an adversary correlates multiple readings from the same source. They propose a correlated differential privacy mechanism tailored to MCS, which takes into account the temporal correlation of sensory data. By adjusting the noise addition process (e.g., adding noise not just to the value but also to the model of the sensor error), their scheme can better protect privacy without overly degrading accuracy. The result is an estimation algorithm that compensates for both the artificial noise and the sensors' inherent errors, producing an accurate aggregate while satisfying DP guarantees. The trade-off is that differential privacy introduces a quantifiable loss in accuracy or utility. In practice, careful tuning of the privacy budget ϵ is needed so that the final application (be it a data analysis or a machine learning model) remains accurate enough while protecting individuals. As privacy regulations tighten and user awareness grows, differential privacy provides a principled way to share aggregated insights from MCS data without exposing specifics of any single contributor.

5.2.4. Homomorphic encryption (HE) and secure computation

While anonymization and perturbation protect privacy by hiding identity or adding noise, HE offers a cryptographic way to protect data exactly by never revealing it in the clear. HE schemes allow arithmetic operations to be performed on encrypted data, producing an encrypted result that, when decrypted, matches the result of operations as if they had been performed on the plaintext. This powerful property enables an MCS server to aggregate or process user-contributed data without ever seeing the raw values. In practice, a commonly used homomorphic encryption in crowdsensing is the Paillier cryptosystem (additively homomorphic): each user encrypts their sensed value with the server's public key and uploads it; the server multiplies all the ciphertexts together (which corresponds to adding the plaintexts) and obtains an encryption of the sum, which it can then decrypt to get the total. Using Paillier or similar additive HE, many aggregation tasks like computing the average, sum, or frequency counts can be done with confidentiality. For example, if users are reporting their step counts or noise level readings, the platform can compute the average noise level by summing encrypted readings and dividing by the number of participants – all without seeing any individual reading in plaintext. This approach was demonstrated by Li et al. [139] in a lightweight aggregation protocol

where smartphones encrypted their data and an edge server aggregated the ciphertexts, achieving high accuracy of results with negligible information leakage. For more complex analyses, such as truth discovery or clustering on crowdsensed data, additive homomorphism may not be enough. Recent works have explored multi-operand or even fully homomorphic encryption in MCS.

A notable example is the BLIND system proposed by Agate et al. [141]. BLIND is a privacy-aware, open-source framework that utilizes homomorphic encryption to perform K-means clustering on the contributed data points securely, grouping data and filtering out outliers without ever decrypting individual contributions. The system ensures that none of the parties (neither the central server nor any proxy) can identify the source of any particular data item, yet the platform can still compute reliable truths (e.g., the most likely true value of a sensed phenomenon) from the encrypted submissions. Achieving this requires carefully designed protocols: BLIND uses an additive HE scheme for aggregation steps and resorts to more advanced techniques for non-linear operations, combined with a secure multi-party protocol for outlier removal. The result is a privacy-preserving computation that is about three times faster than a baseline fully-encrypted approach and yields accuracy (in terms of truth discovery error) within 42 % of a non-private solution. This illustrates the progress in making homomorphic encryption practical for complex MCS tasks, though the computational overhead is still significant. The general architecture for homomorphic encryption in MCS involves each client device performing encryption locally and a server (or servers) doing computations on ciphertexts. Depending on the encryption scheme, the heavy load can be on the server (e.g., fully homomorphic operations are slow) or partially on the client (e.g., generating keys and encrypting large data vectors). Some systems incorporate an edge computing layer to offload encryption tasks. For instance, Wu et al. [143] proposed an edge-assisted HE framework where nearby edge nodes help resource-constrained devices by partially encrypting or translating their data under a homomorphic scheme before forwarding to the cloud. A recent advancement is multi-key homomorphic encryption, which allows data encrypted under different users' keys to be aggregated or computed jointly. Chen et al. [142] introduce a crowdsensing system based on Multi-Functional HE (MFHE), which eliminates plaintext at all stages and permits direct computation on combined ciphertexts from multiple users. They enhance the basic MFHE with techniques like indistinguishability obfuscation and puncturable pseudorandom functions to improve efficiency. The trade-off with homomorphic encryption is clear: it provides strong privacy (data is mathematically confidential), but the performance and complexity costs are high. Fully homomorphic encryption operations can be several orders of magnitude slower than normal operations, and ciphertexts are much larger than plaintexts, leading to communication overhead. Therefore, current deployments often restrict to partial homomorphism (supporting limited operations like addition) or use batching and quantization to simplify computations. Despite these costs, HE is particularly attractive for scenarios where users require confidentiality but still want the community benefits of aggregated data. It removes the need for trust in the server: even if the server is curious or compromised, it cannot read individual data. This level of security is particularly important for sensitive crowdsensing applications in health (e.g., sharing encrypted biomedical signals for analysis) or finance (e.g., aggregate statistics of expenditures). As computing power and cryptographic research progress, we expect to see more real-world trials of HE in MCS. Already, experimental platforms show that basic aggregate statistics over encrypted smartphone data are feasible within practical time frames [139]. For now, many MCS systems choose a hybrid approach, using encryption for the most sensitive parts (like identity or precise values) and lighter techniques for others, to balance security and efficiency.

5.2.5. *Federated learning in crowdsensing*

FL has emerged as a powerful paradigm to protect data privacy by keeping raw data on users' devices and only sharing model updates. In an FL-based MCS system, instead of users sending their sensor readings to a central server for, say, training a machine learning model, the server sends a pretrained model to the users [154]. Each user locally trains that model on their own data (e.g., phone sensor data) and computes an update (such as gradients or weight differences). Then, only the updates – not the raw data – are sent back to the server, which aggregates them (typically by averaging) to improve the global model. This process may iterate for multiple rounds. Because individual data never leaves the device, FL inherently provides a degree of privacy. Google's use of federated learning for the Gboard keyboard (to learn typing patterns without uploading what users type) is a prominent real-world example of this approach, demonstrating its scalability and practicality.

Zhao et al. [138] present CrowdFL, a privacy-preserving MCS system that integrates FL into MCS. In CrowdFL's architecture, a central server (the task publisher) distributes an initial machine learning model to a crowd of participants' devices. The participants use their local sensing data (e.g., Wi-Fi scans, accelerometer readings) to train the model locally, and then upload the model updates (gradients). The server uses a secure aggregation protocol to sum up these gradients and update the global model, without inspecting any individual update directly. This cycle repeats until the model converges. By only exchanging models, CrowdFL mitigates the risk of raw data leakage – an eavesdropper or the server itself sees only numerical weight updates, which are much harder to tie back to specific sensitive information than the raw data would be.

That said, FL is not a silver bullet for privacy. It is known that model updates can sometimes leak information about the training data through sophisticated attacks (e.g., gradient inversion or membership inference attacks). Hence, current research often combines FL with additional privacy measures. One common addition is differential privacy: for example, Ying et al. [155] propose adding calibrated noise to the gradients on each client before sending them out, so that each individual update is differentially private. This ensures that the server cannot confidently recover any single user's contribution, though this comes with some model accuracy loss.

Another line of defense is secure aggregation protocols – cryptographic methods that allow the server to only obtain the sum of all updates, but not any single update in isolation [156]. Google's FL framework implements this so that the server only sees an encrypted aggregate of updates and can decrypt the final aggregated model after enough clients have contributed. Such protocols often use secret sharing or homomorphic encryption: each client shares parts of their update with other clients in such a way that the server can only decode the total. By doing so, even if the server is curious, it cannot inspect one user's gradient. Recent works in crowdsensing apply secure aggregation to protect against malicious or honest-but-curious servers [138].

Another aspect of security in FL-based MCS is robustness against malicious clients. Since the server accepts model updates from potentially unknown devices, there is a risk of poisoned updates (i.e., Byzantine attacks) that could degrade the model or insert false information. Research is ongoing on robust aggregation rules (e.g., median or trimmed mean instead of averaging) to mitigate this, as well as client reputation systems that down-weight suspicious updates. While this strays into security (integrity) more than privacy, it is crucial for real deployments – a federated crowdsensing system for, say, crowdsourced indoor maps must ensure that bad actors cannot distort the learned model. From a system viewpoint, FL introduces communication and computation overhead: models (especially deep neural networks) can be large, and sending frequent updates can strain the network and device battery [157]. Techniques like model compression, update sparsity, and fewer training rounds help alleviate this. In addition, incentive mechanisms are often needed in MCS to motivate users to participate in federated training (given the associated energy and time costs). Some recent frameworks propose reward schemes where users are paid for contributing to model training, with smart contracts on blockchain to ensure fairness [158].

Despite these challenges, the benefit of FL is clear – it fundamentally limits raw data exposure. In fields like indoor positioning, we already see experimental studies where multiple users' phones jointly train a radio signal map model without sharing their raw location-tagged signals, thus protecting user location privacy while still building a useful global model. In summary, FL transforms the MCS architecture by moving data processing to the edge. It works best for scenarios where a predictive model or AI algorithm is the end goal of crowdsensing. When combined with complementary privacy techniques (e.g., noise injection, secure aggregation) and robust design, FL can significantly enhance privacy. The main trade-off is that ensuring privacy in FL (and security against bad updates) can reduce the model's accuracy or the system's efficiency; finding the right balance is a topic of active research. Nevertheless, FL has already seen real-world deployment in commercial systems for privacy-sensitive data collection, which bodes well for its adoption in academic and civic crowdsensing projects.

5.2.6. Blockchain and decentralization

Blockchain technology introduces a fundamentally different paradigm for enhancing security and privacy in MCS by removing reliance on a trusted central authority. In blockchain-based MCS systems, participant interactions, including task announcements, data submissions, and reward disbursements, are recorded on a distributed ledger maintained by a decentralized network of nodes [159]. This ledger is immutable, secured through cryptographic hashing and consensus protocols, and can be made transparently accessible to all stakeholders. This decentralized architecture strengthens both privacy and security as once a transaction (e.g., a user's data submission) is validated and added to the ledger, it becomes permanent and tamper-evident, making any unauthorized modifications immediately detectable. This immutability promotes auditability and enhances the trustworthiness of crowdsensed data. Furthermore, the use of smart contracts, self-executing code embedded in the blockchain, enables automated enforcement of security policies such as data validation and conditional reward release. These mechanisms reduce reliance on centralized backends and increase system resilience against manipulation and failure.

For privacy, a blockchain does not encrypt data by default (indeed, a public blockchain means all data on-chain is visible to everyone), so careful design is needed. One approach is to store only metadata or hashes of the crowdsensed data on-chain, while the actual sensor data is kept off-chain or encrypted. Participants can thus prove that a certain data submission existed (matching a hash on the ledger) without revealing the data to the world. Another approach leverages the pseudonymity of blockchain addresses: users interact with the system through blockchain accounts that need not be linked to their real identity. To strengthen unlinkability, a user could register a new cryptographic address for each task, so that their contributions across tasks cannot be trivially linked. Zou et al. [147] developed CrowdBLPS, a blockchain-based location privacy-preserving crowdsensing system, exemplifying these principles. In CrowdBLPS, the traditional centralized server is replaced by a blockchain network that handles task publishing and data collection in a decentralized manner. Users' location reports are processed through smart contracts that ensure only necessary information (like proof that a user was within a required area) is revealed, and not the exact coordinates. By using cryptographic commitments and threshold secret sharing, their framework ensures that sensitive location information is split among multiple blockchain nodes and only reconstructed when certain conditions are met. This prevents any single node or party from learning an individual's location, addressing the privacy issue while leveraging blockchain for security.

Blockchain is also being used to design privacy-aware incentive mechanisms. A major concern in crowdsensing is how to reward participants fairly while not leaking their identity or contributions. Solutions have been proposed where rewards (payments) are handled in cryptocurrency via smart contracts: for example, a contract can automatically pay a user's blockchain address after they submit valid data. Using techniques like blind signatures, the reward can be claimed by the user without linking the payment to their exact data submission. One such scheme, PARS (Privacy-Aware Reward System) [146], employs a blind signature protocol so that the server signs a "reward token" for a submission, and the user later redeems it on-chain for payment without the system knowing which user got which token. This achieves unlinkability between the data contribution and the reward collection. Blockchain's decentralized consensus also helps prevent fraud and double spending in incentives, a user cannot claim multiple rewards illegitimately because the ledger will record each token use.

The architecture of blockchain-based MCS typically consists of smart contracts that encode the crowdsensing workflow: a contract for task advertisement (with details of data needed and reward offered), a contract for data submission (often verifying that the format or validity criteria are met), and a contract for distributing rewards once submissions are confirmed. Participants and requesters interact with these contracts through transactions. Data verification can be crowd-sourced or automated; for instance, if multiple users report on the same event, a smart contract could cross-verify data consistency before releasing rewards. Privacy enhancements often require extra cryptographic protocols on top of the blockchain: zero-knowledge proofs can be used to convince the contract that "my data meets the requirement" without revealing the data itself. An example is proving you are in region X without revealing your exact location, achieved by zk-SNARKs or range proofs. Some MCS systems integrate trusted execution environments (TEE) with blockchain, where raw data is processed inside secure enclaves and only proof of the processing is written to the chain [145]. This hybrid model, combining blockchain's auditability with TEE's confidentiality, enables decentralized validation and reward distribution without compromising user privacy.

The main trade-offs of blockchain in MCS are performance and complexity. Blockchains (especially public ones like Ethereum) have limited throughput and can incur significant latency (a transaction might take seconds or minutes to be confirmed) and cost (transaction fees). This is problematic for real-time sensing applications or those requiring high data volume. To address this, many solutions use private or consortium blockchains for crowdsensing, which have controlled membership and faster consensus (at the expense of some decentralization). For instance, a city deploying an MCS system might run a consortium blockchain with nodes operated by different departments or companies, thus not fully public but still decentralized among multiple stakeholders. Another strategy is off-chain scaling: only critical events are logged on-chain while bulk data transfer happens off-chain (e.g., using peer-to-peer networks or distributed file systems). Despite these challenges, blockchain brings valuable properties to MCS. It enhances transparency (participants can verify how their data was used and how decisions were made, by inspecting the ledger) and trust (no single authority can quietly manipulate the results or steal data). Early prototypes have shown that a blockchain layer can manage thousands of users' participation records with acceptable overhead for certain use cases [137]. As blockchain technology matures (with improvements like proof-of-stake, sharding, and layer-2 networks), its integration with crowdsensing is likely to become more practical.

5.3. In-depth exploration of existing privacy-preserving mechanisms in crowd-powered IPS

5.3.1. Federated learning-based methods

FL-based decentralized indoor localization has been proposed in [160–163] to enhance user privacy. FL is particularly advantageous when data is sensitive, distributed, or too large to be efficiently centralized. In this paradigm, the model is trained collaboratively across distributed devices, with only the model updates-rather than raw data-being shared and aggregated to improve the global model. This approach ensures that sensitive user data remains on local devices, significantly enhancing privacy and reducing the risk of data breaches. The

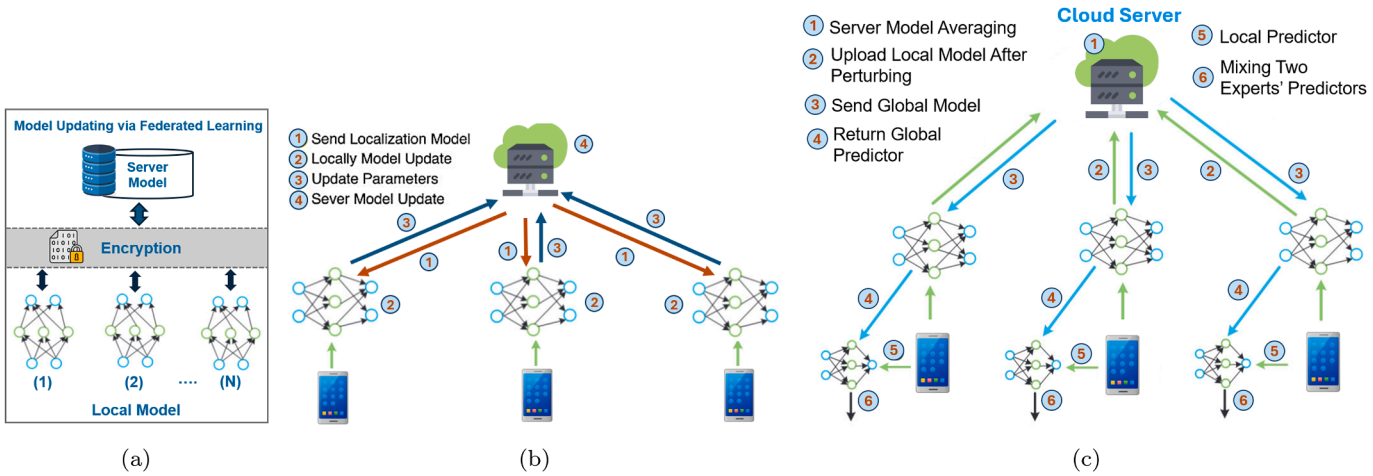

Fig. 13. Comparison of federated learning frameworks for indoor localization: (a) Federated Learning (FLoc), in which a central server aggregates encrypted model updates from multiple clients, updates the global model, and then redistributes it to the participating devices (Reproduced from [164] with permission from Elsevier, © 2025); (b) A more detailed view of the FLoc framework, illustrating its mechanisms for secure model aggregation and distribution (Reproduced from [165] with permission from Elsevier, © 2024); and (c) The Personalized Federated Learning (OPFL) framework proposed by [163] integrates federated learning, differential privacy, and a mixture of experts to enhance privacy preservation and localization accuracy. The cloud server aggregates encrypted model updates from users and provides a global predictor, while local predictors combine with the global model to optimize localization (Reproduced with improved visualization from [163] with permission from IEEE, © 2021).

following subsections delve deeper into specific FL-based approaches, highlighting their mechanisms, challenges, and contributions.

In [160], the framework employs federated weighted averaging to aggregate model updates from multiple users while preserving privacy. The global model update is expressed as:

$$\mathbf{w}^{t+1} = \frac{1}{H}\sum_{u=1}^{n} m_u^t \mathbf{w}_u^t, \quad H = \sum_{u=1}^{n} m_u^t, \tag{36}$$

where m_u^t represents the number of training samples contributed by user u during round t, and $\mathbf{w}_u^t$ denotes the local model weights of user u. This process ensures that no individual user's contributions can be reverse-engineered, thereby preserving their privacy. By focusing on model updates rather than raw data, the FL framework resists data reconstruction attacks that aim to recreate original training data from gradients. Additionally, adaptive learning rates and robust aggregation methods are employed to handle heterogeneous and non-IID data distributions, enhancing privacy guarantees by ensuring that model performance does not disproportionately depend on any single user's data.

In [161], pseudo-labels are generated by the model itself, where the most confident predictions are assigned as labels for previously unlabeled data. The prediction mechanism is defined as:

$$y_i' = \begin{cases} 1 & \text{if } i = \arg\max_{i'} f_{i'}(x) \\ 0 & \text{otherwise,} \end{cases} \tag{37}$$

where $f_{i'}(x)$ is the predicted probability of class i' for sample x, and y_i' is the pseudo-label assigned to sample x. The federated learning component ensures that only model updates, rather than raw data, are transmitted to the server. This is achieved through a federated averaging equation in (36), which aggregates local model updates. By aggregating these updates, the central server enhances the global model without compromising user privacy. The privacy-preserving nature of the framework extends to its resistance against data reconstruction attacks. To optimize global performance, the framework minimizes a federated loss function:

$$L(\omega) = \sum_{k=1}^{K} \frac{n_k}{n} L_k(\omega), \tag{38}$$

where $L_k(\omega)$ is the local loss for client k, n_k is the size of client k's dataset, and n is the total number of samples across all clients. Each client optimizes its local model using stochastic gradient descent:

$$\omega \leftarrow \omega - \eta \nabla l(\omega), \tag{39}$$

where η is the learning rate and $\nabla l(\omega)$ represents the gradient of the loss function. The framework's ability to integrate labeled and pseudo-labeled data ensures robust performance while preserving user privacy. However, challenges such as handling heterogeneous data distributions across devices and ensuring fast convergence remain areas for future exploration. These measures collectively enhance the framework's privacy and security, making it a promising approach for privacy-preserving indoor localization systems.

The FLoc system [162], as illustrated in Fig. 13(a), instead of transmitting raw data to a central server, only encrypted model parameters are shared, significantly reducing the risk of privacy breaches during data transmission. To safeguard these model parameters, FLoc employs homomorphic encryption, which ensures that intercepted updates remain unintelligible to unauthorized entities. This encryption mechanism enables the central server to securely aggregate updates without accessing raw location fingerprints, thereby preserving user privacy. Additionally, the framework integrates horizontal federated learning techniques designed for datasets with the same feature space but distinct samples, allowing the localization model to benefit from diverse user data without directly accessing sensitive information. To strengthen its defense against data reconstruction attacks, FLoc incorporates dropout and noise injection techniques in its deep learning model. These techniques protect against adversarial attempts to infer private information from encrypted updates, ensuring robustness even in challenging security scenarios.

A Privacy-Preserved Online Personalized Federated Learning (OPFL) framework [163], as illustrated in Fig. 13(c), introduces a combination of FL, personalized modeling, and DP to address key challenges in crowdsourced indoor localization. The system integrates DP by injecting artificial Gaussian noise into local model gradients. This ensures that even if gradients are intercepted, they cannot be used to infer private user data. The Gaussian mechanism is defined as:

$$\tilde{g}(x;b) = \frac{1}{b}\sum \left(g(x;b) + \mathcal{N}(0, \Delta s^2 \sigma^2)\right),$$

where $g(x;b)$ is the gradient, b is the batch size, $\mathcal{N}(0, \Delta s^2 \sigma^2)$ represents Gaussian noise with a variance dependent on the global sensitivity Δs, and σ is the noise scale parameter.

To optimize the privacy-accuracy trade-off, OPFL employs a dynamic privacy budget allocation strategy:

$$\epsilon_t = \epsilon_0 e^{-\alpha t},$$

where ϵ_t is the privacy budget for round t, ϵ_0 is the initial privacy budget, and α is the decay factor. This allocation ensures higher privacy protection at earlier rounds when data is scarcer and more sensitive. OPFL also incorporates a Mixture of Experts (MoE) model to balance global generalization and local personalization. The final localization prediction for user i is calculated as:

$$\hat{y}_i = \underbrace{\alpha_i(x) M_G(x, \theta_G)}_{\text{Contribution from the global model}} + \underbrace{(1 - \alpha_i(x)) M_{P_i}(x, \theta_{P_i})}_{\text{Contribution from the personalized local model}}, \tag{40}$$

where M_G and M_{P_i} represent the global and local models, respectively, and $\alpha_i(x)$ is the gating function determined by a sigmoid activation. The architecture is further enhanced by introducing edge computing to offload computational tasks for resource-constrained devices. By leveraging this hierarchical system of cloud and edge servers, OPFL reduces communication latency and optimizes computational efficiency. Through experimental evaluation, OPFL demonstrated significant improvements in localization accuracy while maintaining stringent privacy guarantees. Compared to traditional FL models, OPFL achieved a 20–40 % reduction in localization error under varying levels of noise injection. These results underline OPFL's potential to provide secure, private, and accurate indoor localization services.

5.3.2. Cryptographic-based methods

Conventional fingerprint-based localization schemes often expose sensitive RSS data to the service provider, leading to potential privacy breaches. To address this, the study in [166] introduces a privacy-preserving framework for fingerprint-based indoor localization by leveraging Paillier homomorphic cryptography (PHC) to protect user data during location determination. Homomorphic encryption enables mathematical operations to be performed directly on encrypted data, ensuring that location computations are carried out without revealing the underlying RSS values. The localization process is divided into three phases: preparation, distance computation, and location retrieval. In the preparation phase, the client device encrypts its scanned RSS values, $V' = (v'_1, v'_2, \ldots, v'_N)$, and prepares them for secure transmission to the server. For each RSS value, the client computes:

$$S_2^{\text{comp}} = \{-2v'_1, -2v'_2, \ldots, -2v'_N\}, \tag{41}$$

and

$$S_3 = \sum_{j=1}^{N} \left(v'_j\right)^2, \tag{42}$$

before encrypting and transmitting $[[S_2^{\text{comp}}]]$, $[[S_3]]$, and the corresponding public key. During the distance computation phase, the server calculates the squared Euclidean distance between the encrypted client RSS values and the fingerprints stored in the database. This process is defined as:

$$[[d_i]] = [[S_{i,1} + S_{i,2} + S_3]] = [[S_{i,1}]] \cdot [[S_{i,2}]] \cdot [[S_3]], \tag{43}$$

where

$$[[S_{i,1}]] = \left[\left[\sum_{j=1}^{N} v_{i,j}^2\right]\right], \tag{44}$$

$$[[S_{i,2}]] = \left[\left[\sum_{j=1}^{N} (-2v_{i,j} \cdot v'_j)\right]\right]. \tag{45}$$

In the location retrieval phase, the client decrypts the received distances and determines the k-nearest neighbors. The final location is computed as the weighted centroid of these neighbors, where the weight w_i for each neighbor is defined as:

$$w_i = \frac{1 - \left(d_i / \sum_{j=1}^{k} d_j\right)}{k - 1}. \tag{46}$$

The proposed framework ensures strong privacy guarantees by encrypting all client data before server interaction, preventing unauthorized access or inference of user locations. Furthermore, the use of crowd-sourced fingerprint data enables scalability and adaptability to dynamic environments. Compared to traditional methods, the framework significantly reduces computational overhead through novel filtering techniques such as Fingerprint Similarity Filtering (FSF) and Known AP Filtering (KAF), enhancing both efficiency and localization accuracy.

To ensure robust privacy preservation in fingerprint-based localization systems, [167] introduces a secure crowdsourced framework leveraging cryptographic mechanisms. The core concept of the framework is illustrated in Fig. 14, where a central server facilitates encrypted communication and task management between data requesters and contributors. The system workflow consists of several stages: (1) task request and key generation, (2) public key delivery, (3) encrypted distance upload, and (4) winner selection. This ensures the privacy of contributors' sensitive data while maintaining localization accuracy. The framework incorporates also Paillier homomorphic encryption to perform essential mathematical operations directly on encrypted data. This preserves the privacy of both the contributors and the requesters during sensitive computations. The encrypted distance $E(d_i)$ between the reported location and the target is computed as:

$$E(d_i) = Enc(d_i, pk), \tag{47}$$

where the function Enc represents an encryption algorithm that secures the Euclidean distance d_i using the public key pk. Specifically, $\text{Enc}(d_i, pk)$ encrypts d_i such that only authorized entities with the corresponding private key can decrypt it. This process ensures the confidentiality of the data during transmission or storage. The decryption process to retrieve the final result is handled securely by the central server using the private key sk, expressed as:

$$d_i = Dec(E(d_i), sk), \tag{48}$$

ensuring that contributors' raw data remains protected throughout the computation. To further enhance privacy, the system includes a mechanism for encrypted sensing data exchange, payment processing, and winner selection based on proximity to the target. The overall process minimizes privacy risks while ensuring fairness and efficiency in task allocation. The cryptographic privacy-preserving approach addresses security concerns and builds trust among participants, making it a scalable solution for modern IPSs.

5.4. In-depth exploration of existing security-preserving mechanisms in crowd-powered IPS

5.4.1. BERT-ADLOC: secure localization against adversarial attacks

The BERT-ADLOC system [168] introduces a robust approach to address privacy and security concerns in crowdsourced IPS by detecting and mitigating adversarial attacks during the fingerprint database update phase. As illustrated in Fig. 15, the system categorizes attacks into four types:

- **Attack I:** Random generation of fingerprints without knowledge of legitimate beacons, using random MAC and RSSI generators.
- **Attack II:** Generation of fingerprints with knowledge of valid beacon data, exploiting the legitimate beacon list.
- **Attack III:** Manipulation of existing fingerprints by adding random noise.
- **Attack IV:** Mislabeling fingerprints with incorrect location labels from a legitimate database.

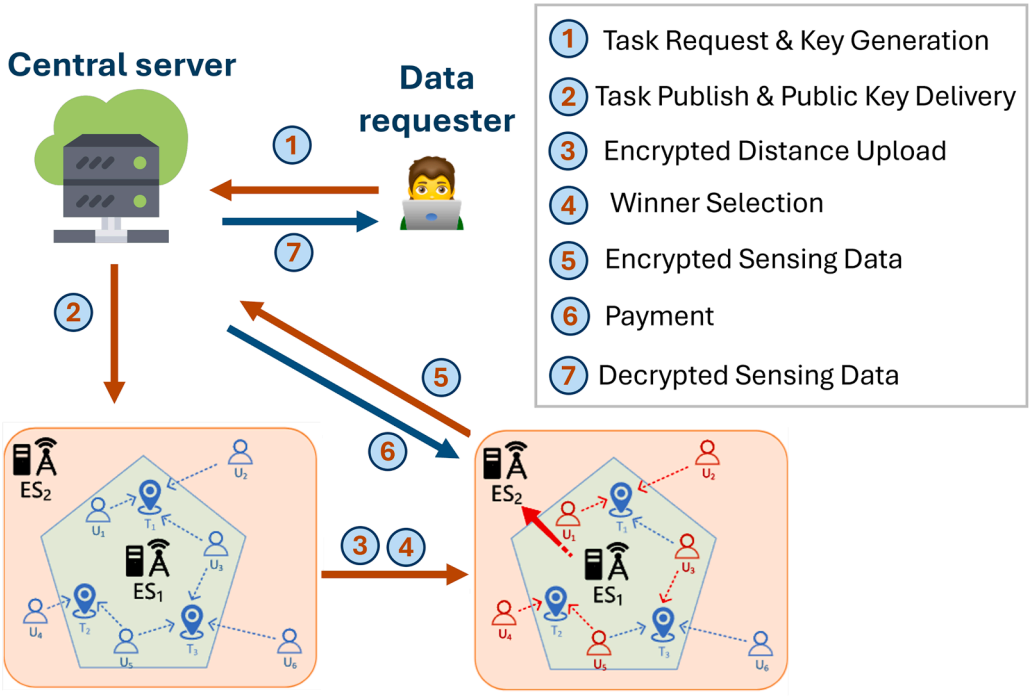

Fig. 14. Overview of the Privacy-Preserving Crowdsourced Localization Framework (PPCF) proposed by [167], which is based on homomorphic encryption. The process involves the following steps: First, the *Data Requester* sends a task request to the *Central Server*, which generates and distributes the necessary public key. The *Central Server* then publishes the task to the environment and provides the public key to participants (e.g., users $U_1, U_2, \ldots, U_n$). Participants compute their distances to the task target and upload these distances in encrypted form to the server. The server evaluates the encrypted distances to determine the winner (e.g., the user with the closest or most appropriate location). (Figure reproduced with improved visualization from [167] with permission from Elsevier, © 2022).

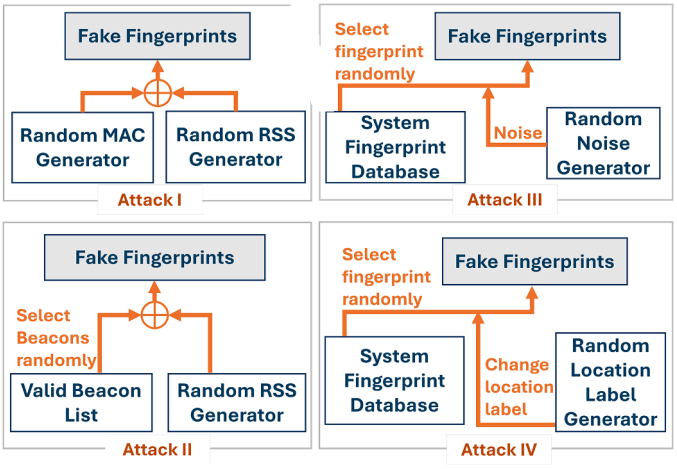

Fig. 15. Overview of attack types during the fingerprint database update phase. (Figure reproduced from [168] with permission from Elsevier, © 2021).

To counter these attacks, the BERT-ADLOC system incorporates two components: the Adversarial Sample Discriminator (BERT-AD) and the Indoor Localization Model (BERT-LOC). BERT-AD uses a self-attention mechanism to detect counterfeit fingerprints during database updates, while BERT-LOC safeguards against online attacks by identifying malicious beacons and legitimate beacon manipulations. The discriminator evaluates the authenticity of fingerprint data using a binary cross-entropy loss function:

$$L_{\text{AD}} = -\frac{1}{N}\sum_{i=1}^{N}\Bigg[\underbrace{y_i \log(p_i)}_{\substack{\text{Logarithmic penalty for} \\ \text{incorrect predictions of legitimate samples}}} + \underbrace{(1-y_i)\log(1-p_i)}_{\substack{\text{Logarithmic penalty for} \\ \text{incorrect predictions of fake samples}}}\Bigg], \tag{49}$$

where y_i represents the true label (1 for legitimate samples, 0 for fake samples), p_i is the predicted probability assigned to the legitimate class, and N denotes the total number of samples. The loss function ensures the accurate classification of legitimate and adversarial samples by penalizing errors proportionally to their likelihood, thereby enhancing the robustness of the system against attacks. For indoor localization, the BERT-LOC model estimates the location of legitimate fingerprints while rejecting manipulated data. Its training objective minimizes the localization error:

$$L_{\text{LOC}} = \frac{1}{M}\sum_{j=1}^{M}\left\|\mathbf{l}_j - \hat{\mathbf{l}}_j\right\|_2^2, \tag{50}$$

where $\mathbf{l}_j$ is the true location of fingerprint j, $\hat{\mathbf{l}}_j$ is the predicted location, and M is the total number of fingerprints. To ensure data integrity during the update phase, BERT-ADLOC employs a joint optimization framework:

$$L_{\text{Joint}} = \underbrace{\alpha L_{\text{AD}}}_{\substack{\text{Adversarial detection contrib.}}} + \underbrace{\beta L_{\text{LOC}}}_{\substack{\text{Localization accuracy contrib.}}}, \tag{51}$$

where α and β are weighting factors balancing adversarial detection and localization accuracy. BERT-ADLOC leverages BLE RSS fingerprints, which are inherently privacy-sensitive. By training the system with robust self-attention mechanisms and latent feature extraction, the model improves its ability to generalize across diverse attack scenarios. This enables real-time detection and mitigation of adversarial activities during both the database update and online phases. In summary, the BERT-ADLOC system integrates adversarial detection and robust localization to safeguard crowdsourced IPS against diverse attack types. Its use of ad-

vanced deep learning methods, such as BERT-based models, enhances scalability, accuracy, and resilience in real-world scenarios.

5.4.2. Abnormal crowd traffic detection (ACTD) scheme

The ACTD scheme [47] addresses critical privacy and security challenges in WiFi fingerprint-based IPSs by detecting abnormal crowd traffic and mitigating adversarial behaviors in crowdsourced environments.

The scheme focuses on three levels of attacker models:

- **Level 1 Attacker:** Individual pseudonymized users attempting to misrepresent RSS measurements.
- **Level 2 Attacker:** Collaborative groups of users engaging in coordinated behaviors to manipulate location data.
- **Level 3 Attacker:** Advanced adversaries using spoofed RSS data and collusion with access points (APs) to disrupt localization accuracy.

Each level is addressed using specific detection mechanisms to preserve data integrity and ensure system reliability. The core privacy-preserving strategy involves the use of pseudonyms to anonymize user identifiers. Each user is assigned a unique pseudonym (pid_i) during data collection and transmission to safeguard their identity. However, pseudonyms alone are insufficient to defend against sophisticated attackers. To strengthen security, ACTD incorporates a Pseudonym Scoring Mechanism (PSM), which evaluates user behavior based on RSS patterns. A scoring function is defined as:

$$c_i = \frac{1}{T}\sum_{t=1}^{T} \text{Dev}(RSS_t),$$

where c_i is the confidence score for user i, T is the total number of RSS samples, and $\text{Dev}(RSS_t)$ measures the deviation of RSS samples from expected values. To detect collusion among users (Level 2), the system employs a Pattern Similarity Tree (PST) approach. PST models the RSS patterns submitted by users and identifies anomalous correlations indicative of coordinated attacks. The detection threshold for collusion is dynamically adjusted using:

$$H = \gamma \cdot \text{Sim}(RSS_k, RSS_j),$$

where $\text{Sim}(\cdot)$ represents the similarity metric between users k and j, and γ is an adaptive parameter. For Level 3 attackers, who exploit AP organizers, ACTD integrates a distance metric learning approach to differentiate genuine and spoofed RSS data. The final stage involves outlier detection, which identifies anomalous RSS values by comparing them to historical fingerprints in the database. Outliers are flagged and removed to prevent disruption in IPS localization services. ACTD further ensures user privacy by decoupling RSS data from physical identities and anonymizing AP identifiers during the data aggregation process. By focusing on pseudonym-based anonymization, ACTD prevents attackers from inferring sensitive user information. Moreover, its hierarchical detection architecture enhances system security by addressing adversarial behaviors at multiple levels. In summary, the ACTD scheme offers a robust solution to privacy and security challenges in crowdsourced IPSs. By combining pseudonym anonymization, collusion detection, and outlier analysis, it effectively counters adversarial attacks while preserving user privacy. Experimental evaluations demonstrate significant improvements in detection accuracy and localization robustness compared to baseline methods, highlighting ACTD's potential in real-world applications.

5.4.3. Reputation-driven fog-assisted secure crowdsourcing framework (RDF-SCF)

The RDF-SCF framework proposed in [127] provides a robust solution to privacy and security challenges in crowdsourcing-based IPS. As shown in Fig. 16, RDF-SCF leverages a fully trusted fog server platform that acts as an intermediary between service requesters and responders. This platform ensures secure interactions by monitoring communication channels and reducing vulnerabilities associated with direct data exchanges. A key feature of RDF-SCF is its reputation-based incentive mechanism, which dynamically adjusts reputation scores to reward honest and reliable responders while penalizing malicious actors. By prioritizing trustworthy participation, this mechanism discourages adversarial behaviors. To counter collusion attacks, RDF-SCF employs game-theoretic strategies to model interactions between attackers, responders, and the fog server. The replicator dynamic equation is used to analyze the evolution of responder behaviors and identify stable equilibrium states:

$$\dot{x}_i = x_i\left(\frac{U_i}{\bar{U}} - 1\right), \tag{52}$$

where x_i represents the proportion of responder i's contributions, U_i denotes the utility of responder i, and $\bar{U}$ is the average utility of all responders. This equation ensures that responders providing higher-quality contributions are incentivized, while malicious behaviors are penalized. The platform's adaptive strategies dynamically respond to the severity of collusion attacks, quantified by the collusion degree (λ), allowing for real-time adjustments in monitoring and penalties. The utility of responders is further modeled to balance incentives and penalties, as follows:

$$U_r = P_r - C_r + \text{Reputation Adjustment}, \tag{53}$$

where P_r is the payment received, C_r represents the cost incurred by the responder, and adjustments are determined by reputation dynamics. By integrating these adaptive and dynamic components, RDF-SCF ensures the sustainability of social welfare while maintaining the integrity of IPS operations. This comprehensive approach combines fog computing, reputation-based incentives, and game-theoretic modeling to establish a scalable, secure, and trustworthy framework for crowdsourced indoor navigation.

5.5. Gaps in existing approaches

The security and privacy mechanisms in crowdsourced IPS present a range of strengths and weaknesses, each addressing specific challenges. Table 10 categorizes the mechanisms based on their technical approach, concisely highlighting their advantages and challenges. While BERT-ADLOC [168] demonstrates robustness against diverse adversarial attacks by employing advanced deep learning techniques, it struggles with high computational demands and requires retraining for new attack types. In contrast, ACTD [47] effectively detects coordinated attacks and preserves user anonymity through pseudonym-based mechanisms, but its sensitivity to noise in data collection and performance overhead in dynamic environments limit its adaptability. On the other hand, RDF-SCF [127] overcomes scalability issues by leveraging fog computing and incentivizing honest contributions through a reputation-based system. However, it depends on a trusted fog infrastructure and remains vulnerable to large-scale malicious collusion. Unlike these, FL-based privacy mechanisms [160–163] decentralize model training to ensure strong privacy and adaptability to heterogeneous data distributions, yet they face difficulties with non-IID data and impose significant computational and communication overhead. Lastly, cryptographic-based privacy frameworks [166,167] provide unparalleled mathematical guarantees for data security through homomorphic encryption, making them highly resilient to data reconstruction attacks. However, their computational overhead and limited scalability hinder their practical implementation in large-scale systems. Together, these mechanisms highlight a trade-off between robustness, efficiency, and scalability, necessitating further innovation to achieve comprehensive solutions in crowdsourced IPS.

5.6. Concluding remarks

Several approaches have been proposed to enhance privacy and security in crowd-powered IPS, including cryptographic safeguards to

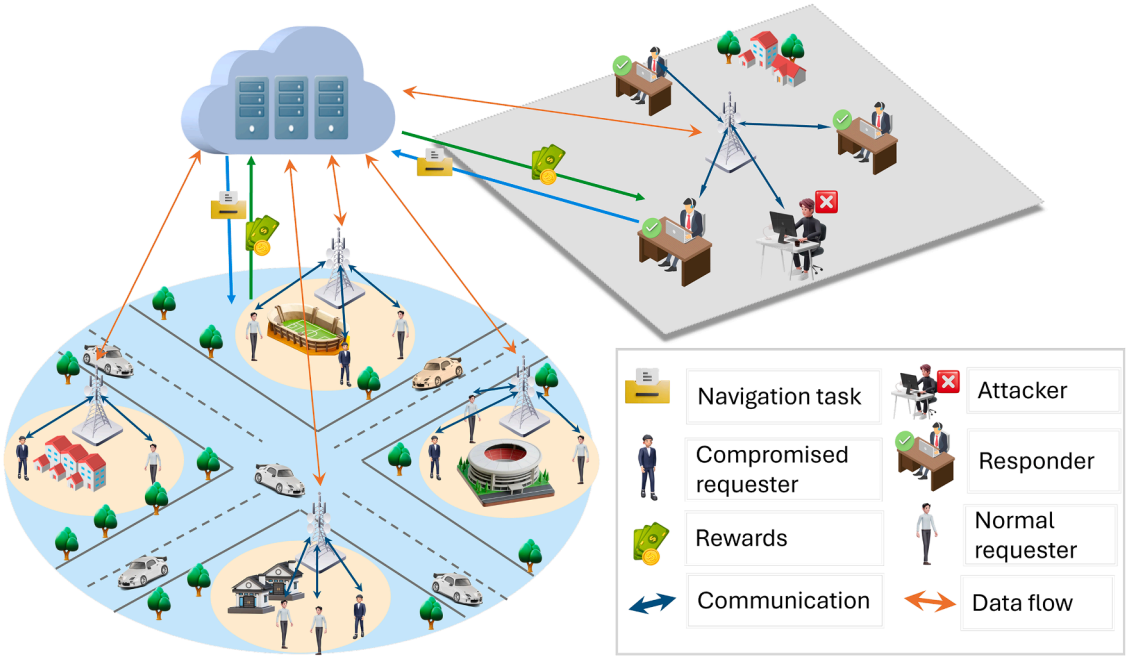

Fig. 16. Visualization of the RDF-SCF framework from [127,169], highlighting the fog server platform's role in enabling secure transactions, implementing reputation-based incentives, and deploying adaptive strategies to counter collusion attacks. (Figure inspired and generated with improved visualization from [127,169] with permission from Elsevier, © 2022).

Table 10
Summary of security and privacy mechanisms in crowd-powered IPS.

Mechanism	Description and Technical Approach	Advantages and Challenges
BERT-ADLOC: Secure Localization Against Adversarial Attacks [168]	Detects and mitigates adversarial attacks on fingerprint databases using a joint adversarial sample discriminator (BERT-AD) and localization model (BERT-LOC). Employs loss functions to penalize adversarial samples and optimize localization accuracy.	**Advantages:** Robust against diverse attack types; ensures data integrity during updates. **Challenges:** Computationally intensive; retraining needed for unseen attacks.
Abnormal Crowd Traffic Detection (ACTD) [47]	Implements pseudonym-based anonymization and attacker detection using deviation scoring, Pattern Similarity Trees (PST), and outlier analysis.	**Advantages:** Detects coordinated attacks; preserves anonymity. **Challenges:** Sensitive to data noise; overhead in dynamic environments.
Reputation-Driven Fog-Assisted Framework (RDF-SCF) [127]	Leverages fog computing and a reputation-based incentive model. Uses game-theoretic methods to detect and penalize malicious users.	**Advantages:** Scalable via fog architecture; incentivizes honest behavior. **Challenges:** Requires trusted infrastructure; vulnerable to mass collusion.
Federated Learning (FL)-Based Privacy Mechanisms [160–163]	Decentralizes training; only model updates are shared. Techniques include differential privacy, encryption, and personalized learning.	**Advantages:** Strong privacy guarantees; adaptable to heterogeneous data. **Challenges:** Non-IID data reduces performance; communication and compute overhead.
Cryptographic-Based Privacy Frameworks [166, 167]	Uses homomorphic encryption for secure computation on encrypted data, especially in distance calculations and task selection.	**Advantages:** Mathematical privacy guarantees; protects against data reconstruction. **Challenges:** Heavy computational cost; scalability issues with large datasets.

protect data confidentiality, federated learning to enable decentralized model training without exposing raw data, anomaly detection for identifying malicious or abnormal behaviors in real time, blockchain-based trust frameworks to ensure data integrity and accountability, and incentive-compatible designs that align user participation with secure and privacy-preserving practices. Collectively, these methods address diverse threats that arise across the MCS lifecycle. Existing solutions demonstrate considerable progress but reveal persistent trade-offs between computational efficiency, scalability, and the robustness of protection, underscoring the need for adaptive, context-aware frameworks. As the following section explores, these protective mechanisms are not isolated from the user experience-rather, their computational, communication, and energy costs directly influence device performance, battery longevity, and overall user participation, making it essential to examine the operational impact of IPS data collection and localization on end-user devices.

Table 11
Smartphone sensor characteristics: sampling rates, power consumption, and typical uses.

Sensor	Sampling Rate (Hz)	Power Consumption (mA)	Typical Uses
GNSS	1	100	Outdoor localization
Wi-Fi Scanner	0.1–1	40	Indoor localization
Cellular Network	On-demand	<2	Broad area positioning
Accelerometer	10–200	0.5	Motion detection, PDR
Gyroscope	10–200	6	Orientation tracking
Magnetometer	10–50	1	Heading estimation
Barometer	1–10	0.5	Floor level detection
Light Sensor	0.5–10	0.1	Ambient environment detection
Proximity Sensor	On-demand	0.01	Interaction (e.g., screen off during calls)
Microphone	8,000–48,000	5–20	Audio recognition, sound analysis
Camera	30 and more (video)	200–300	Visual positioning, AR

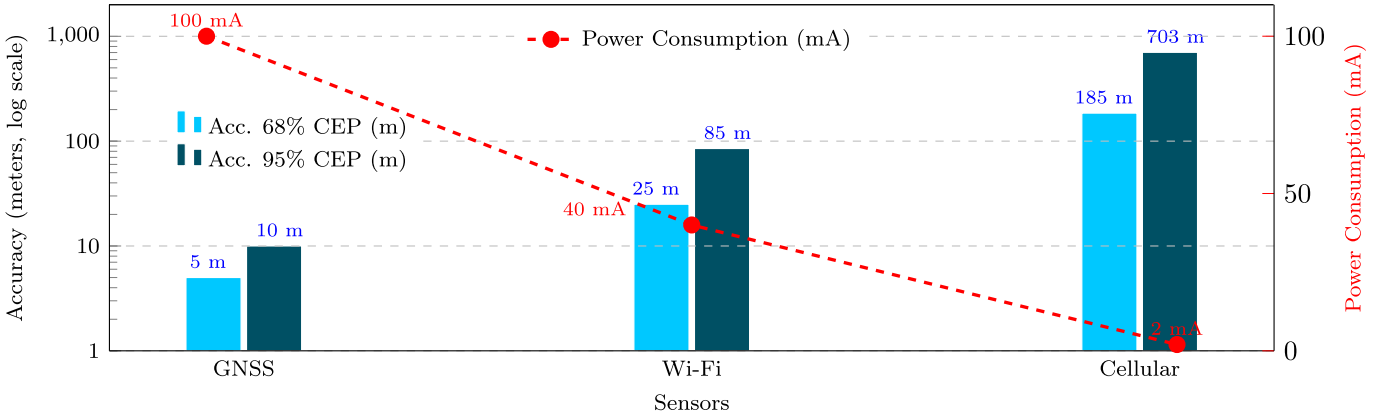

Fig. 17. Comparison of accuracy and power consumption for GNSS, Wi-Fi, and cellular positioning methods. CEP stands for Circular Error Probable. The values for accuracy and power consumption are adapted from Huawei's presentation at the IPIN 2024 conference [170].

6. Impact of collection and localization on users' devices

Despite the incentives provided and privacy measures implemented, the potential adverse effects of data collection and localization processes on users' devices cannot be ignored. Prolonged or resource-intensive processes can lead to device performance degradation, such as increased battery consumption, storage utilization, or processing delays. These issues may result in user fatigue, diminished engagement, or eventual withdrawal from participation in crowdsourced data collection efforts. This section examines the implications of data collection and localization on device performance, considering scenarios where these processes are executed locally on the device versus offloaded to a centralized server (Table 11).

6.1. Resource consumption during data collection

Crowd-powered localization relies on the sensors in users' smartphones, such as GNSS, Wi-Fi, cellular signals, and IMUs, to gather data critical for accurate positioning [171]. However, this process imposes significant demands on energy, storage, and network resources, impacting smartphone performance and user experience.

Energy consumption is a primary concern, with high-frequency GNSS sampling consuming up to 100 mA, Wi-Fi scanning at 40 mA, and cellular localization at 2 mA, as shown in Fig. 17. Continuous operation of these sensors, particularly GNSS, drains batteries quickly, making long-term use unsustainable without adaptive strategies like on-request activation or reduced sampling frequency. *Data transmission* adds further strain, particularly when large volumes of sensor data are uploaded to servers. High-resolution GNSS traces or Wi-Fi signal maps consume significant bandwidth, further intensifying battery drain under weak connectivity conditions. Background transmissions amplify these effects, often causing unexpected energy depletion and reduced device responsiveness. *User preferences and device settings* further shape the effectiveness of data collection and transmission. Battery-saving modes or disabled location services, often employed to conserve energy, restrict data collection frequency and transmission capability. In parallel, privacy-aware users may limit sensor permissions or restrict background data access, reducing the quality and quantity of crowdsourced data available for aggregation. *Storage constraints* also pose challenges, especially for older devices or those with limited capacity. Dense sensor data, such as detailed GNSS traces or Wi-Fi maps, quickly accumulate, risking interruptions in data collection without real-time compression or filtering. To address these constraints, optimizing data pipelines via adaptive sampling, lightweight compression, and context-aware sensor scheduling is essential, ensuring energy-efficient and user-friendly localization systems.

6.2. Impact of localization processes

Localization processes exert a considerable influence on energy efficiency, device responsiveness, and positioning accuracy. This impact can be analyzed across two dimensions: *always-on vs. on-request systems* and *device-based vs. server-based processing*.

6.2.1. Always-on vs. on-request systems

Always-on systems continuously operate sensors for real-time tracking, as shown in Fig. 17. GNSS offers high accuracy (5–10 meters) but consumes substantial power (100 mA), Wi-Fi provides moderate accuracy (25–85 meters) with lower power consumption (40 mA), and cellular localization has low accuracy (185–703 meters) but is highly energy-efficient (2 mA). These systems are suitable for applications requiring uninterrupted localization, but their high energy consumption, particularly for GNSS and Wi-Fi [172], renders them unsuitable for prolonged use without frequent recharging. In contrast, *on-request systems* activate sensors only when needed, significantly reducing energy usage. This approach is ideal for scenarios requiring periodic updates, but it comes

with trade-offs, such as activation latency and potential accuracy reductions due to sensor recalibration after idle periods.

6.2.2. Device-based vs. server-based processing

Device-based processing handles all computations locally, increasing energy and processing demands on the device. These demands are especially pronounced in always-on systems, while on-request systems mitigate them at the cost of responsiveness. *Server-based processing* offloads computations, reducing device-side energy consumption but increasing reliance on network connectivity. This introduces latency, potential privacy risks, and elevated bandwidth consumption, particularly in environments with unreliable networks. Hybrid approaches, such as edge computing, offer a middle ground by balancing the trade-offs between local and remote processing.

6.3. Existing mitigation strategies

Efficient data collection in crowd-powered IPS necessitates strategies that minimize resource consumption on user devices while ensuring accurate and timely updates to the radio map database. Fig. 18 illustrates a framework proposed in [35] that addresses these challenges through a context-aware design. The framework is built upon three key decision layers, each targeting a specific dimension of environmental and user context: radio map availability, motion behavior, and indoor/outdoor status.

1. *Radio Map Availability:* Upon initiating a data collection task, the system determines whether a radio map for the current area already exists. If no such map is available, the system enters an initial construction mode to generate a new radio fingerprint database. Otherwise, it employs an incremental update mechanism to refine the existing map based on newly acquired data.
2. *Motion Mode:* To adapt to user activity, the system classifies motion states into static or walking. When the user is in motion, a dynamic tracking strategy is invoked to capture temporal and spatial variations in the signal environment. Conversely, if the user is stationary, a low-overhead collection mode is employed to conserve battery life and processing resources.
3. *Indoor/Outdoor Detection:* Environmental awareness is critical for tailoring data acquisition intensity. Indoor settings, characterized by complex multipath propagation and higher signal variability, require continuous and fine-grained measurements. In contrast, outdoor environments are typically more stable and thus permit reduced sampling rates to conserve resources.

By integrating these three layers of contextual adaptation, the framework achieves a balanced trade-off between localization fidelity and resource efficiency. The resulting data collection strategies enable reliable updates to the radio map while minimizing disruption to the user's device performance.

6.4. Gaps and limitations of current literature

Despite the progress made in addressing user-related challenges in crowd-powered IPS, there remains a significant gap in the literature addressing the mitigation of the data collection effect on user contribution. Most existing studies, including the work proposed in [35], focus on general data collection strategies but lack tailored solutions for balancing energy efficiency, data quality, and system reliability in diverse real-world scenarios. A notable limitation of the above mentioned framework is its reliance on predefined motion modes and environmental contexts without considering dynamic or unpredictable user behavior, such as erratic movement patterns or abrupt environmental changes. Additionally, while the framework proposes strategies to adjust data collection rates, it does not account for heterogeneous devices with varying sensing and computational capabilities, which may lead to uneven performance across users. Privacy concerns are another critical limitation, as continuous data collection, even with optimized strategies, may raise concerns about user trust and data security. Furthermore, the lack of mechanisms for adaptive learning and real-time adjustment to unexpected user behaviors or environmental shifts restricts the scalability and robustness of current approaches. These gaps highlight the need for further research into more flexible, user-centric mitigation strategies that can dynamically adapt to diverse contexts while maintaining high system efficiency and user satisfaction.

6.5. Concluding remarks

To set the stage for translating design principles into real-world impact, this section has examined how data collection and localization processes affect user devices in crowd-powered IPS. While adaptive sampling, hybrid processing architectures, and context-aware strategies offer promising mitigation pathways, key challenges persist. These include managing energy and storage constraints, accommodating device heterogeneity, addressing unpredictable user behaviors, and preserving user trust. The absence of fully dynamic, user-adaptive strategies remains a limiting factor in current solutions. To explore how these challenges manifest and are addressed in practical settings, the next section turns to large-scale real-world deployments. These case studies provide grounded insights that inform a roadmap of design recommendations, research directions, and potential breakthroughs for future IPS systems.

7. Real-world case studies, roadmap of recommendations, future research directions, and potential breakthroughs

7.1. Case studies of real-world deployments at a scale

Over the past decade, crowd-powered IPS have garnered significant attention from both academia and industry, resulting in their growing integration into large-scale mobile ecosystems. Recognizing the economic and practical value of IPS technologies, major technology providers, including Google, Apple, and Huawei, have embedded IPS functionalities into their flagship LBS, such as Google Maps, Apple Maps, and Huawei Maps, which collectively serve millions of users daily. Notably, Google reported in 2013 that Google Maps alone supports over one billion users per month. Maintaining the accuracy and freshness of such services remains a persistent challenge, given the dynamic and complex nature of real-world indoor environments. To address this, commercial providers increasingly rely on crowdsourcing methods that exploit users' sensor-equipped smartphones for data collection and map refinement. Modern mobile devices, equipped with Wi-Fi modules, inertial sensors, and positioning capabilities, serve as ubiquitous sensing platforms that bridge the physical and digital domains, enabling continuous and scalable environmental monitoring. Due to their low deployment and maintenance costs, crowd-powered IPS have emerged as a practical and scalable solution for enhancing indoor LBS and enabling seamless navigation experiences. In this section, we review selected case studies that exemplify the real-world deployment of crowd-powered IPS, demonstrating their technical feasibility, operational scalability, and increasing relevance in ubiquitous positioning infrastructures. We further analyze each system's deployment scale, user participation model, performance outcomes, and the strategies employed to ensure scalability, adaptability, and user-centric design.

7.1.1. Passive user intervention scheme proposed by Huawei Edinburgh Research Centre (ERC) for calibration-free radio map construction

A significant development in scalable Wi-Fi-based IPS involves the recent approach proposed by the ERC group [173], focusing on calibration-free radio map construction through graph map matching. This approach addresses critical limitations of traditional manual site surveys and heavily supervised data collection by employing a crowdsourced methodology with minimal user intervention. Users contribute

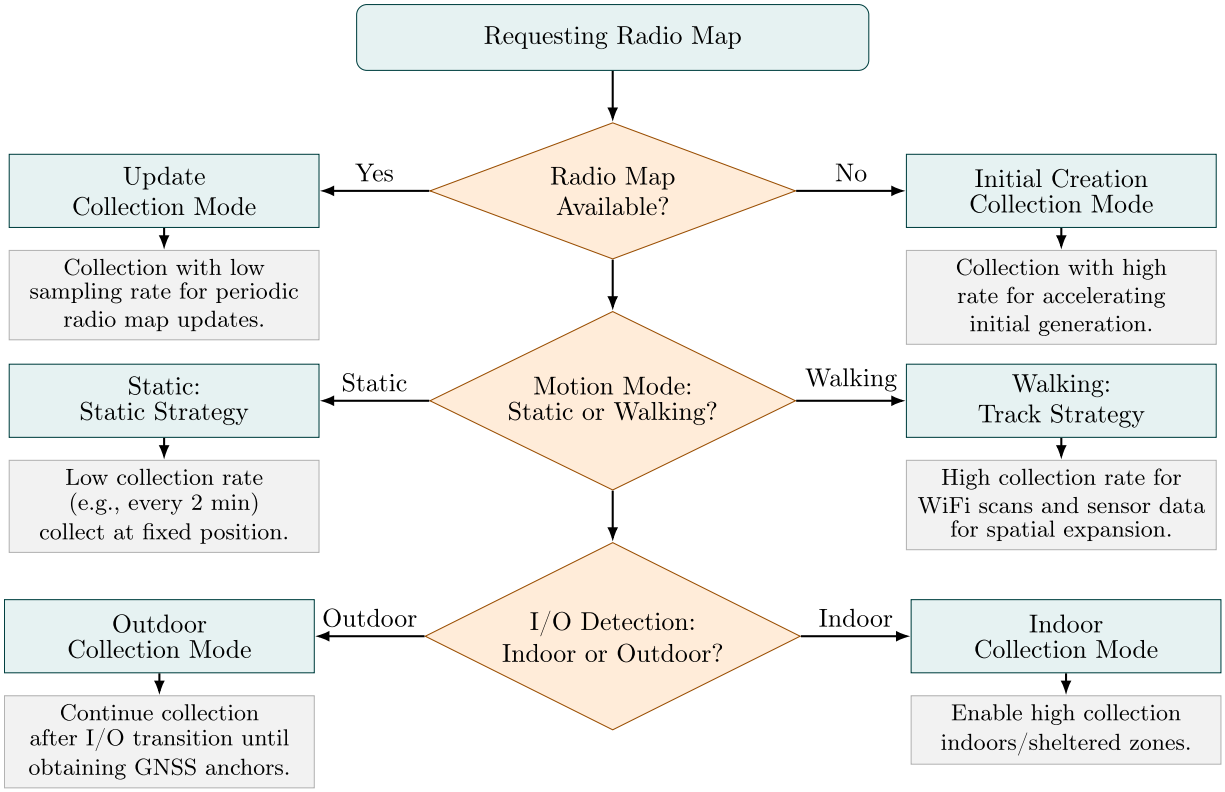

Fig. 18. Flowchart for context-aware data collection strategy and key considerations proposed in [35] to reduce the impact of data collection on smartphone performance, including indoor/outdoor (I/O) environmental awareness, radio map existence, and user motion modes (Figure redesigned by the authors to visualize strategies inspired by [35] with improved visualization and clarity).

by naturally walking within indoor environments. At the same time, their smartphones collect sensor data such as Wi-Fi signals and inertial measurements, thus requiring no explicit calibration or controlled positioning from users.

To empirically test this methodology, *pseudo-crowdsourced data* were collected through approximately 200 trajectories at the ERC, 4th floor. Each trajectory lasted roughly two minutes, with no enforced requirements regarding phone location or orientation, resulting in realistic and diverse data collection scenarios. The data included common PDR noise factors, such as varying phone orientations, handheld, backpack, or pocket, as well as Wi-Fi noise, including interference from mobile hotspots. Data collection involved three distinct models of Huawei smartphones. Additionally, real crowdsourced data gathered from Huawei mobile phone users in 2022 was incorporated, characterized by a complete lack of control over device orientation and positioning, thereby exhibiting even higher PDR noise levels. This broader dataset spanned distinct floors in prominent shopping locations, such as the Joy City mall in Beijing, the Global Harbor mall in Shanghai, and the Vientiane World shopping centre in Shenzhen. The study by Hughes et al. [173] encompassed extensive empirical evaluation across these diverse indoor venues, totaling 26 floors. The large-scale testing leveraged thousands of crowdsourced trajectory estimates to construct comprehensive and accurate Wi-Fi radio maps. Their implementation involves a two-stage optimization process: an initial unsupervised trajectory alignment based on Wi-Fi and PDR relationships, followed by refined graph matching and map deformation optimization. This effectively mitigates inaccuracies inherent in traditional radio map methods, such as sequential placement constraints and dependence on highly accurate indoor maps.

Performance results demonstrated consistently robust and reliable positioning accuracy. Specifically, in typical office settings, the system achieved median localization errors as low as 1.3 meters using a particle-filter-based recursive algorithm and 2.2 meters using the single-shot WKNN algorithm. In more complex, open-area mall environments, these methods maintained median errors of approximately 4.6 meters (particle filter) and 8.1 meters (WKNN). These empirical findings affirm the practical viability and adaptability of crowd-powered IPS, which achieves competitive accuracy without requiring explicit user calibration. Such performance highlights the potential for scalable deployment in diverse and dynamic indoor spaces.

7.1.2. *Large shopping malls aided By BLE beacons (MLoc in China)*

One notable example of deploying IPS at scale is the MLoc system, successfully implemented in numerous large shopping malls across China [174]. This commercial deployment highlights critical considerations regarding user involvement and infrastructural decisions to balance system reliability, scalability, and user convenience. In contrast to conventional Wi-Fi-based fingerprinting approaches, MLoc deliberately employs BLE beacons in combination with geomagnetic field (GMF) signals for localization. This choice was primarily driven by the limitations associated with Wi-Fi signal usage, including irregular scanning frequencies on Android devices, API restrictions on iOS platforms, and periodic MAC address changes for privacy. Consequently, MLoc deployed a network of battery-powered BLE beacons at strategic locations, such as ceilings along corridors and atriums within malls. Typically, beacon spacing ranged from 10 to 15 meters in general areas, with denser placement, approximately 6 meters, used in challenging environments (e.g., large open atriums) to improve fingerprint uniqueness and positioning accuracy. However, the adoption of BLE beacons introduces a significant trade-off concerning user roles. While BLE beacon infrastructures substantially reduce active user participation, thus lowering user intervention and operational burden, they simultaneously require initial physical installations, periodic maintenance (battery replacement and hardware repairs), and strategic spatial planning. In contrast, traditional Wi-Fi fingerprinting opportunistically utilizes existing infrastructure without additional hardware installation or maintenance costs.

Yet, Wi-Fi-based IPS typically necessitates more intensive user calibration and suffers reliability issues stemming from heterogeneous device behaviors and privacy-driven limitations, as evidenced by diminished scanning frequency and limited API access.

MLoc's design thus mitigates these reliability challenges by incorporating limited but critical user roles through a landmark-based crowdsourcing approach. Human collectors visited pre-defined landmarks, capturing BLE and GMF fingerprints with precise ground-truth labeling. Although the approach still demands user intervention, the targeted and well-structured landmark selection effectively balances manual labor with accuracy and scalability [43]. Further optimization was achieved by generating recommended collection paths to reduce collectors' workload, enhancing both data quality and efficiency. Despite the successful deployment of BLE beacons in MLoc, replicating this strategy across all building types remains questionable due to practical limitations. While malls, airports, and hospitals might feasibly adopt BLE infrastructure given their economic incentives and operational capabilities, widespread BLE deployment in residential, educational, or small-scale commercial buildings would face significant economic and logistical barriers. Conversely, Wi-Fi infrastructures, already pervasively deployed, continue to offer a more feasible alternative for large-scale, passive localization efforts despite their inherent reliability drawbacks. Overall, MLoc's implementation illustrates an effective compromise between reducing user intervention and ensuring positioning reliability via targeted BLE beacon deployment combined with minimal structured user engagement. Nevertheless, the broader applicability of BLE-based infrastructure across diverse indoor environments remains more constrained compared to the universally present and opportunistically exploitable Wi-Fi networks.

7.1.3. Campus-wide multi-building deployment

Complementing mall-based deployments like MLoc, academic studies have provided substantial insights into the scalability and practical viability of Wi-Fi-based IPS through campus-wide implementations. A noteworthy example of such a deployment is presented by Jaisinghani et al. [175], who leveraged existing Wi-Fi infrastructure for server-side indoor localization across a large university campus. This deployment covered seven major buildings comprising a total of 38 floors, utilizing an extensive and well-established Wi-Fi infrastructure consisting of hundreds of dual-band APs managed through 11 controller clusters. Having been operational for over four years and supporting thousands of daily connections, this infrastructure provided an ideal foundation for deploying an IPS without requiring additional hardware installations. Notably, the system was designed as a server-side localization solution specifically to minimize user involvement. Instead of requiring user-installed apps or device-level modifications, which often hinder user adoption, this approach passively collected RSSI data directly from the Wi-Fi AP controllers. Consequently, users experienced no disruption or additional requirements, as any Wi-Fi-connected device could be passively localized using only signal strength data. However, a carefully defined user role was essential, involving approximately 200 landmarks strategically surveyed over a three-week period by system implementers to establish an accurate fingerprint database for system evaluation and operational reference. The server-side IPS achieved effective room-level accuracy, typically within a few meters. The deployment of heuristic refinements markedly enhanced localization performance compared to baseline approaches, particularly under conditions of high positioning uncertainty. This campus-wide implementation highlights the feasibility of utilizing existing infrastructure and passive crowd-derived signal data for large-scale, multi-building Wi-Fi IPS deployments. Importantly, the minimal user intervention approach facilitated broad accessibility and adoption, underscoring the practicality and attractiveness of passive, infrastructure-centric IPS solutions.

7.1.4. Summary and concluded remarks form real-world case studies

Real-world case studies from 2020 to 2025 demonstrate that Wi-Fi fingerprinting-based IPS can be effectively scaled to large, densely populated indoor environments while maintaining practical levels of accuracy. Several key lessons emerge from these deployments. Chief among them is the strategic utilization of existing infrastructure, particularly widespread Wi-Fi installations, and the MCS potential of users who naturally traverse these spaces. Equally important is addressing user-centric challenges, such as ensuring seamless app adoption and accommodating the diversity of user devices, through thoughtful and adaptive system design choices. In commercial settings such as shopping malls, hybrid crowd mapping strategies combined with multi-sensor fusion (e.g., BLE and geomagnetic signals) have enabled reliable navigation services for millions of users [174]. In institutional environments such as university campuses and airports, infrastructure-based approaches that leverage Wi-Fi controller data or deploy lightweight sensors have demonstrated the feasibility of large-area coverage with minimal active user participation [175]. Collectively, these real-world deployments affirm that crowd-powered Wi-Fi IPS is no longer a conceptual prototype but a viable and scalable solution for complex indoor environments. The consistent success of these systems illustrates that with deliberate user-centric design and infrastructure-aware implementation, Wi-Fi-based IPS can deliver robust, scalable performance.

The subsequent section suggests a roadmap of recommendations for developing user-friendly crowd-powered IPS solutions. These guidelines are derived from an in-depth synthesis of recent research advancements and observed from large-scale real-world deployments.

7.2. Recommendation for scalable crowd-powered IPS

It is evident that user-centric challenges in crowd-powered IPS are not only interrelated but also mutually dependent, such that addressing one issue often necessitates resolving others. Developing the next generation of crowd-powered IPS requires a cohesive and holistic approach to these challenges, this forms the basis of our first recommendation. In what follows, we propose a set of actionable guidelines aimed at enabling user-friendly, scalable, and sustainable crowd-powered IPS design and deployment.

7.2.1. Recommendation for user-friendly involvement

To enhance user participation in crowdsourced IPS, a *hybrid approach combining passive and active engagement* is highly recommended. Below are the key strategies and considerations:

1. Contextual Prompts and User Personalization: User time and differences in preferences between users should be respected and considered to attract contributions. Thus, the following points should guide the engagement design:
   - *Contextual Prompts*: Design prompts that are contextually relevant and time-sensitive, such as during periods of low activity. By ensuring that prompts are well-timed and pertinent, the likelihood of user annoyance is reduced. Studies on crowdsourcing app engagement emphasize that thoughtful design of content submission features improves user participation and retention [176].
   - *User Control and Personalization*: Providing users with the ability to customize their interaction preferences, such as the frequency and type of prompts, fosters greater satisfaction and long-term engagement. Personalized options ensure users feel in control, leading to sustained participation and higher retention rates, as noted in prior research [176].
2. AI-Driven Analysis-Based Unobtrusive Active Engagement: Active user interactions inspired by brief, minimally intrusive prompts popularized by platforms such as YouTube, Meta (Facebook), and Google Maps have demonstrated significant real-world success in maintaining user engagement. YouTube's use of concise, context-driven prompts enables users to effortlessly choose related content or explore new topics, enhancing viewing duration and satisfaction [177].

Examples of such prompts on YouTube include: "*Do you want to keep watching videos for this topic?*" or "*Would you like to explore more from this creator?*" Similarly, Meta's Facebook platform successfully integrates unobtrusive notifications and questions directly within the user's browsing flow, allowing seamless interaction without disruption [178]. Typical questions that appear on Facebook include: "*Are you interested in this reel?*", delivered in a format that users can easily skip or respond to without leaving their current activity. In navigation applications, such as Google Maps' crowdsourced transit notifications [179], users efficiently provide real-time feedback on crowd density without interrupting their navigation or browsing experience. A typical unobtrusive prompt might be: "*How crowded was your bus?*" or "*Was there available seating during your ride?*" In the context of indoor positioning and annotation, adopting this proven approach ensures interactions remain brief, context-aware, and non-disruptive. AI-driven analysis enhances this by intelligently generating concise and personalized prompts, considering the user's current location, immediate surroundings, and activity context (e.g., identifying the specific building, floor, or nearby landmarks). Such AI-powered notifications optimize timing and relevance, improving both response quality and user experience. Examples of contextually optimized, unobtrusive notifications include:

- *Building and Coarse 2D Location Annotation:* Prompts can request users to confirm or annotate building-level details and coarse 2D locations. For instance, prompts may support tasks such as location matching, building identification and labeling, or annotating a user's position relative to specific areas within a building. See Fig. 19(A) for examples of location matching prompts. Fig. 19(B and D) also illustrates how users can annotate the main part of a building, or a building. User responses link sensed Wi-Fi and magnetic signatures with the correct building boundaries and provide meaningful semantic labels, such as building names, wings, or main sections. This process enhances the accuracy of building identification, particularly in densely built environments where GNSS errors frequently extend beyond actual building boundaries.
- *Enhanced Localization Using Semantic Labels*: Users can provide semantic details for specific areas, enriching the system's indoor maps. For example, Fig. 19(D) illustrates building identification prompts, while Fig. 19(C) presents additional annotation examples that can be used to annotate shops, offices, and POI. These user confirmations link sensor readings to real-world locations and labels, improving both localization accuracy and map granularity.
- *Floor Calibration and Absolute Labeling*: Short notifications can confirm floor-level information, helping to refine altitude and pressure-based algorithms. For instance, refer to Fig. 19(E). These simple queries help the system adjust its detection methods and improve future user experiences.

3. Semantic Annotation from User Input for Navigation: When a user searches for a specific destination, such as classroom F1201, the navigation process can simultaneously contribute to the collection of radio and magnetic signatures. By linking these signatures to the user's path and their final arrival at the destination, the system improves the accuracy of indoor positioning. This approach works effectively in both active and passive user scenarios, as detailed below:
   - *Active User Case*: The system can explicitly involve the user by prompting them to confirm their arrival at a specific location. For example, when a user reaches classroom F1201, the system may ask for confirmation:

Have you arrived at classroom F1201?

     When the user confirms the location, the system records the associated radio and magnetic signatures and links them directly to that specific spot. This user input plays a key role in fine-tuning the localization process, ensuring that the recorded data is accurately matched to the correct room. Over time, this method enhances the detail and accuracy of the indoor map, making it more reliable and precise.
   - *Passive User Case*: The system employs background data collection to infer a user's arrival at a specific location. By analyzing contextual cues, such as reduced movement patterns, alignment of the user's trajectory with predefined paths, and sensor data (e.g., Wi-Fi signals or magnetic field variations), it can determine that the user has arrived at a location like classroom F1201 without requiring active input. Once the arrival is inferred, the system automatically records the associated radio and magnetic signatures, along with the time spent at the location. This passive approach minimizes user involvement while still allowing the system to annotate and localize collected data effectively. Over time, it complements active user engagement by contributing data from a wide range of scenarios, thereby creating a more detailed and accurate indoor map. It is critical, however, to implement passive data collection strategies that do not burden users. Factors such as privacy, security, battery life, hardware capabilities, and device temperature must be carefully considered. For instance, the study in [120] proposes methods to reduce the potential negative impacts of data collection on user experience (see Fig. 18).

By integrating both active and passive strategies, the system can optimize the balance between user effort and data accuracy. Active confirmation ensures high-confidence localization in critical areas, while passive methods enable seamless data collection in routine navigation scenarios. Together, these approaches improve the semantic annotation of indoor spaces, creating a robust and scalable IPS.

7.2.2. Recommendations for effective incentive strategies

Designing effective incentive strategies for crowdsourced IPS involves balancing user motivation with the diverse *system goals* (i.e., localization reliability, cost, availability, data quality, sustainability, and ubiquity).

1. *Aligning incentive types with system goals*: The types of incentives, such as reputation systems, gamification, social incentives, and financial rewards, should be selected and tailored based on the system goals, as referred to in Section 4.4.2. Sustained engagement requires minimal financial costs [180]. Reputation systems effectively foster trust and credibility by awarding scores or badges that recognize contributors' quality and reliability, encouraging consistent participation and supporting reliability and sustainability [58]. Tying IPS contributions to personal fitness goals, such as walking or exercise, enhances both enjoyment and productivity [72,101,181]. By aligning these goals with gamified tasks, such as route annotation or area coverage, platforms can tap into users' intrinsic motivation, making recruitment easier and participation more satisfying [182]. Social incentives further boost engagement by fostering community and validation. Group contributions to shared maps, public recognition, or friendly competitions, like logging steps or covering areas, motivate users while promoting health [72]. Finally, financial rewards provide direct incentives for high-effort tasks, such as mapping sparsely covered spaces [70,72]. However, monetary rewards must be balanced to prevent over-reliance or reduced engagement when removed.
2. *Tailoring to cultural and demographic diversity*: Incentive strategies must account for the cultural and demographic diversity of users. As discussed above, incentives should align with cultural norms [183]. For instance, non-monetary rewards like public recognition may resonate more in collectivist societies, while material rewards might be more appealing in individualistic contexts [183]. Strategies must also cater to varying motivations among demographic groups; for example, younger users may respond well to gamification, while professionals might prefer reputation systems or intellectual satisfaction [184]. Additionally, affordability can be maintained by em-

(A) Location Matching (B) Coarse Location Context (C) Semantic Labels and POI

(D) Building Identification Prompts (E) Floor Absolute Labeling

Fig. 19. AI-driven and context-aware suggested user prompt categories designed to enable unobtrusive, concise, and time-sensitive active engagement for labeling crowdsourced data. These prompts support semantic annotation tasks such as building identification, floor labeling, and POI tagging.

ploying low-cost or no-cost incentives, such as collaborative challenges or public acknowledgments, ensuring scalability in resource-constrained environments.

3. *Fostering intrinsic motivation and societal impact*: Intrinsic motivators, such as the desire to contribute to societal benefits [185], play a significant role in user participation. Highlighting the collective impact of user contributions, such as improving accessibility or supporting emergency services, fosters a sense of ownership and purpose [186]. Privacy-preserving frameworks, like federated learning, further strengthen trust by ensuring that users maintain control over their data while contributing to the system. This combination of societal value and trust-building measures enhances user engagement and long-term participation.
4. *Communicating value and purpose*: Effectively communicating the value and purpose of user contributions is critical to fostering consistent engagement [187]. When users understand how their efforts improve navigation systems, enhance accessibility, or contribute to urban planning, they are more likely to participate regularly [185]. Clear communication not only increases participation but also ensures the reliability and quality of the collected data, ultimately contributing to the system's success and scalability.
5. *Adaptive incentive mechanisms*: The adaption is essential to address user diversity and evolving system requirements. These mechanisms dynamically adjust incentive structures by considering various factors, such as user preferences, demographics, and geographic contexts. They also align with system goals, such as improving data coverage in low-traffic areas or ensuring data reliability in high-demand zones. By leveraging real-time feedback and user behavior, machine learning or optimization techniques can be employed to refine strategies over time. For example, adaptive mechanisms might use gamification [188] to engage urban users while offering financial rewards to incentivize participation in rural or sparsely covered regions. This flexibility ensures that incentive strategies remain both scalable and cost-efficient.

7.2.3. Recommendations for enhancing privacy and security

Building upon the mechanisms and gaps identified in Table 10, we propose the following recommendations to inform the development of more robust, scalable, and resource-efficient security and privacy solutions for crowd-powered IPS.

1. *Augment Robustness with Explainable AI (XAI):* Adversarial detection frameworks (e.g., BERT-ADLOC [168]) might benefit from explainable AI methods to illuminate how attacks are identified and why certain samples are flagged; refer to [189] for more details on XAI methods. This transparency could assist human operators in refining rules, diagnosing false positives, and tracing novel attack patterns. Integrating XAI would further strengthen user trust and facilitate regulatory compliance in privacy-sensitive applications such as hospital patient tracking or personalized navigation for individuals with disabilities.
2. *Enhance Cross-Framework Interoperability:* Current approaches often focus on a single technical domain (e.g., purely FL-based or purely cryptographic). A hybridized solution would enable systems to employ, for instance, FL-based training for coarse modeling and homomorphic encryption for high-stakes operations such as user authentication or distance calculations [166]. This multi-layered architectural design can accommodate varying threat levels while maintaining a balanced trade-off between computational overhead and security guarantees.
3. *Develop Adaptive Defense Mechanisms:* Advanced adversaries can dynamically evolve their attack vectors or collusion strategies over time, particularly in open and dynamic crowdsourcing settings. Adaptive defenses, such as the joint training of adversarial sample discriminators [168] and crowd traffic anomaly detectors [47], should be regularly updated using recent data. Incorporating model retraining or continual learning mechanisms can ensure these defenses remain effective against evolving threats.
4. *Foster Transparent Reputation and Incentive Systems:* Reputation-driven frameworks (e.g., RDF-SCF [127]) effectively encourage honest participation but often rely on fully trusted intermediaries or fog nodes. To bolster transparency, future systems could integrate audit trails or distributed ledger technologies (DLTs) to log participant behaviors, ensuring that reputation scores and incentives cannot be tampered with. This approach would reduce the risk posed by collusive groups and untrusted service providers.
5. *Incorporate Privacy by Design for Large-Scale Deployments:* Scalability constraints are a recurring challenge in cryptographic frameworks [166,167] and multi-device FL [160,162]. To address these limitations, system architects should adopt a "privacy by design" principle-emphasizing efficient data structures, modular cryptographic routines, and on-demand encryption. Edge computing resources could be leveraged to handle computationally heavy tasks in smaller batches, thus minimizing latency and energy consumption in large-scale networks [190].
6. *Standardize Attacker Models and Evaluation Criteria:* Multiple studies adopt different attacker definitions and threat levels (e.g., random fingerprint generation, collusion, or adversarial manipulation). Establishing community-wide benchmarks and standardized attacker models (Level 1–3 as in [47], for instance) would enable more consistent, comparable evaluations. Future work should also specify metrics that jointly measure privacy preservation, system accuracy, and computational overhead, thereby providing a balanced assessment of proposed techniques.

By adopting these recommendations, researchers and practitioners can more effectively address the diverse and evolving privacy and security challenges in crowdsourced IPS. Moving beyond singular, domain-specific defenses to multifaceted, adaptive frameworks will be pivotal for ensuring both user trust and system resilience in real-world deployments.

7.2.4. Recommendations to mitigate the impact of data collection and localization process

Regarding the impact of data collection, crowdsourced localization systems employ several strategies to balance energy efficiency, data quality, and user satisfaction [23]. *Adaptive sampling* dynamically adjusts data collection rates based on user context, increasing sampling during movement and reducing it when stationary. In contrast, *low-power sensing* prioritizes energy-efficient sensors like magnetometers and cellular RSS to minimize energy consumption during prolonged data collection. *Battery-aware operations* align data collection with device battery levels [39], enabling intensive collection at high levels and low-power modes when the battery is low [191,192]. *Intelligent transmission scheduling* batches data uploads during periods of strong connectivity or low network congestion, reducing energy use and bandwidth consumption. *Efficient data management*, through compression, filtering, and optimized storage, limits transmission and storage overhead, ensuring device responsiveness [17,193]. *Environmental awareness*, such as indoor/outdoor differentiation, prioritizes GNSS outdoors and low-power sensors indoors, reducing redundant data collection. *Optimized radio map updates* use high sampling rates during initial mapping and periodic low-frequency updates to balance resource usage over time, while *user motion-based strategies* adjust collection frequency based on activity, with static users requiring minimal updates and dynamic users benefiting from higher rates. *Context-aware Wi-Fi scanning* adapts scan rates to mobility and environmental conditions, conserving energy in stable environments while maintaining accuracy in dynamic ones. Finally, *context-aware data management*, including geofencing and behavioral analysis, reduces redundancy, and *user incentives*, such as gamification and rewards, sustain engagement while promoting energy-efficient practices.

As for the localization process, mitigating the impact of localization processes on device performance requires integrating advanced techniques that balance energy efficiency, accuracy, and responsiveness. *Efficient localization algorithms* rely on low-power sensors and data fusion methods to deliver precise positioning with minimal resource demands. *Hybrid localization techniques* dynamically combine GNSS, Wi-Fi, Bluetooth [194], and low-power sensors like magnetometers and light sensors, prioritizing the most efficient method based on the environment to optimize both energy use and accuracy [35]. *Edge computing* offloads intensive tasks to local servers or base stations [195], reducing device-side resource consumption [196] while maintaining low latency and scalability [197]. *Synergistic Integration of MCS with Fog Computing for IPS:* In addition to edge computing, integrating MCS with complementary architectures such as fog computing offers additional benefits for large-scale, real-time deployments. Fog computing extends computation and storage capabilities to proximate network nodes (e.g., access points, routers), enabling data processing closer to the source. This proximity yields several advantages for IPS. First, latency is reduced because location estimates and environmental updates can be computed locally, an essential feature for time-sensitive indoor navigation and tracking applications. Second, fog nodes can incorporate fine-grained contextual and environmental information (e.g., floor maps, local interference patterns) into real-time inference, thereby improving positioning accuracy. Third, computation and data storage loads are distributed between fog nodes and the cloud: fog handles localized inference, while MCS frameworks coordinate broader-scale analytics and adaptive task allocation. Finally, in large or multi-building deployments, the distributed nature of fog infrastructure enhances scalability and resilience, ensuring continuity even when parts of the network experience outages or congestion. Such an integrated architecture, combining the precision and context-awareness of fog computing with the adaptability and scalability of MCS, presents a promising direction for future IPS deployments. *Low-Power Indoor and Outdoor Detection (IOD)* systems such as [35,198] leverage multi-signal fusion from barometers, magnetometers, and light sensors to achieve detection accuracy of 99 % with minimal power consumption, addressing the challenge of seamless transitions in location-based services. For instance, modern IOD systems target a power increase of less than 1 mA and algorithm delays under 1 s, enabling continuous operation without degrading device performance [170]. Together, these strategies create a robust framework for sustainable, scalable localization systems that enhance user satisfaction and maintain high performance in resource-constrained environments. Together, these strategies-efficient algorithms, hybrid methods, fog edge computing and processing, and advanced IOD, create a robust framework for sustainable, scalable localization systems that enhance user satisfaction and maintain high performance in resource-constrained environments.

7.3. Unified theoretical framework integrating user-centric factors

Building on the preceding recommendations, the proposed unified framework (illustrated in Fig. 20) synthesizes a broad range of user-centric input factors, including user attributes, device states, environmental context, and system-level constraints, into a cohesive, adaptive decision-making engine. Rather than treating engagement, incentives, and privacy in isolation, the framework holistically processes these interdependent factors to drive system-level adaptations. For example, real-time user-related inputs (e.g., a user's current activity, preferences, or fatigue) are considered alongside device status (battery level, sensor availability), environmental context (location type, time, or ambient conditions), and provider-side requirements (urgency of data needs or network constraints). By cross-referencing these domains, the framework can dynamically adjust its strategies in a coordinated manner. This means that decisions on incentive management, participation mode, and privacy controls are made jointly and synergistically.

An adaptive incentive module, for instance, leverages these inputs to personalize rewards or motivations in real time, offering higher incentives or alternative types when user motivation is low or device burden is high, and scaling back when intrinsic engagement is detected, thus implementing personalized and adaptive incentive strategies. Simultaneously, the framework's participation control toggles between active and passive user involvement based on context: it intelligently switches to unobtrusive passive sensing when a user is busy or environmental conditions are unsuitable for interaction, and only prompts active participation through brief, context-aware requests when it can be done unobtrusively and to high effect. This realizes the goal of contextual and unobtrusive user engagement by ensuring that any user interruption is minimal and well-timed.

In parallel, a contextual privacy management component continuously adjusts data handling policies (e.g., data granularity, anonymity level, or consent prompts) according to the user's privacy preferences and situational sensitivity. By making privacy context-aware (for instance, automatically enhancing privacy safeguards in sensitive environments or when users indicate a higher level of concern) and transparent (clearly communicating what data is used and giving users control), the framework upholds user trust without stifling data collection. Crucially, all these decisions feed into each other: for example, if stricter privacy controls reduce the available data, the system may respond with different incentives or engagement tactics to maintain performance, illustrating how the components cooperate rather than work at cross-purposes.

In operationalizing the interdependence of engagement, incentive, and privacy considerations, this unified framework ensures that crowd-powered IPS adaptations are cohesive and user-centered. Such integration enhances usability (by tailoring the system's behavior to the user's context and device capabilities, reducing frustration and effort), trust (by respecting privacy and transparency, thereby encouraging continued participation), and scalability (by sustaining user participation and data quality across diverse scenarios).

Beyond technical and engagement dimensions, the financial overhead associated with launching and maintaining a crowdsensing campaign presents a significant barrier to large-scale IPS deployment. These costs may encompass participant recruitment, incentive provisioning, device resource consumption, and campaign coordination. Without careful planning, expenses can escalate-particularly in long-term or wide-area deployments. Simulation environments offer a practical and cost-effective approach to addressing this challenge by enabling the testing and optimization of task assignment strategies, coverage planning, and data quality control prior to real-world implementation. Such pre-deployment evaluations can help identify inefficiencies, optimize resource allocation, and ultimately reduce the overall operational burden.

Ultimately, this unified user-centric approach serves as a practical roadmap for hybrid participation models in crowd-powered IPS, wherein adaptive incentives, context-aware engagement, and privacy safeguards are orchestrated together to achieve a more resilient and user-friendly system.

7.4. Future research directions and potential breakthroughs to enhance crowd-powered IPS

Building upon the insights offered by the unified theoretical framework and the substantial progress made by both academic and industrial communities in addressing user-centric challenges in crowd-powered systems, this section identifies and stresses on key future directions and potential technological and methodological breakthroughs that, if realized, could significantly advance the effectiveness and scalability of crowd-powered IPS.

1. Consent-Aware UIs and Trust-Scoring for Transparency: A common challenge is user distrust or misunderstanding of how their data is used. A forward-looking solution involves consent-aware user interfaces that dynamically reflect what data is being collected, how it is anonymized, and how it contributes to the system. Complemented by a trust score, a visual indicator of how well the system respects user

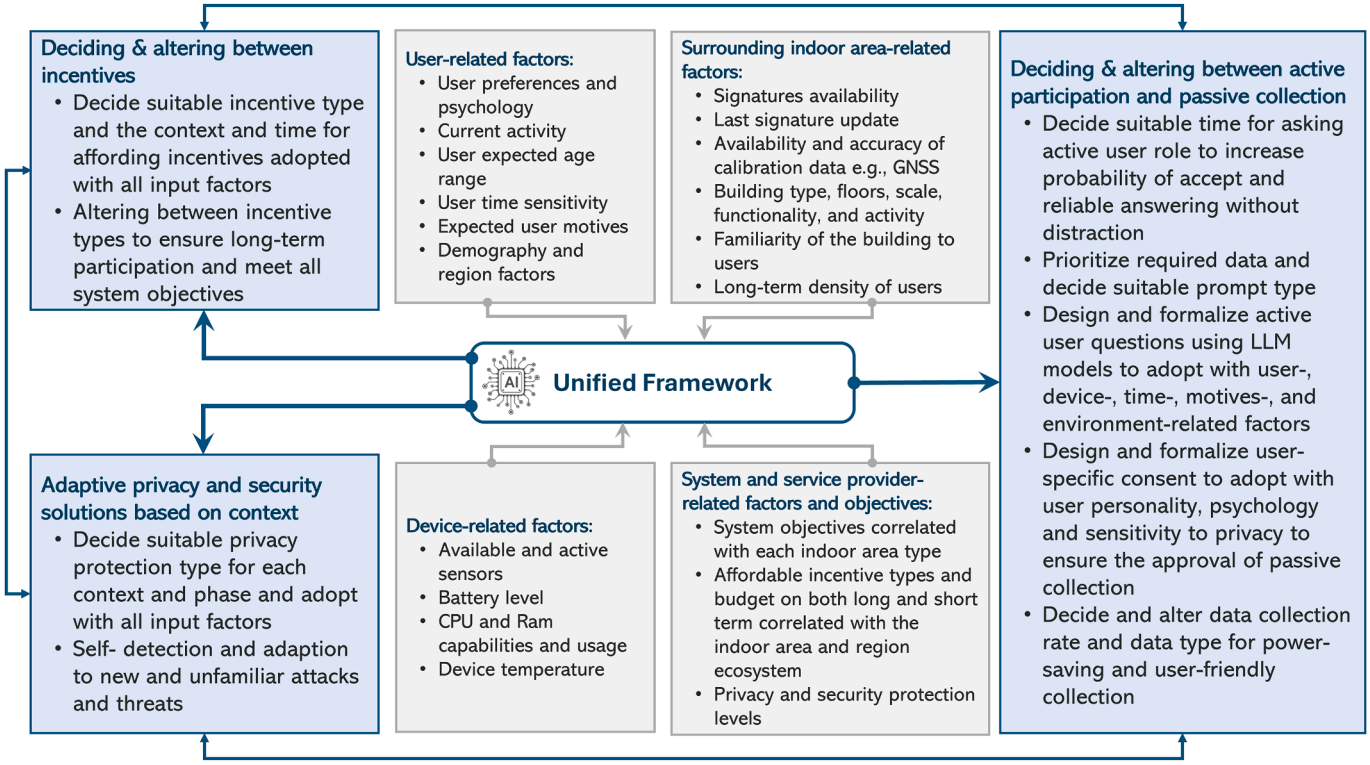

Fig. 20. A unified framework for user-centric crowd-powered IPS. The framework dynamically integrates user-, device-, environment-, and provider-related factors to adaptively manage incentive schemes, participation modes (active and passive), and privacy-preserving mechanisms. By leveraging real-time context and AI methodologies, it can simultaneously make intelligent decisions on when and how to prompt users, assign incentives, and enforce privacy safeguards, ultimately enhancing usability, trust, and system scalability.

preferences over time, such interfaces empower users to take control of their data. These can be further integrated with privacy dashboards that provide interactive summaries of what data was used, deleted, or retained. This feedback loop directly addresses transparency and informed participation, increasing user confidence and long-term engagement.

2. Context-Aware Micro-Incentives for Just-In-Time Unobtrusive Active Engagement: One barrier to crowd participation is the perceived irrelevance or poor timing of data collection requests. Future crowd-powered IPS can adopt context-aware micro-incentive and active user participation systems that trigger only when user context is favorable, e.g., low movement speed, high battery, stationary activity. Coupled with micro-payments or social rewards, these well-timed requests feel less intrusive and more aligned with user behavior. Importantly, such systems can learn each user's preferred engagement window, forming personalized sensing profiles that optimize data quality while minimizing burden. This increases engagement efficiency and reduces dropout due to annoyance or distraction.
3. Quantitative Assessment of User-Centric Factors on Crowd-Powered IPS Performance: A key future research direction involves the systematic and quantitative assessment of trade-offs between different user involvement modalities, such as active, passive, and opportunistic participation, and their impact on positioning accuracy, data volume, and system scalability. This includes the design of controlled experimental studies that normalize key environmental variables (e.g., building layout, access point distribution, and device heterogeneity) to enable fair and comparable evaluations across deployments. Indirect engagement metrics, such as participation rate, session duration, and response frequency, could be extracted from system usage logs to infer user interaction levels and behavior patterns. Complementarily, structured user surveys embedded within navigation applications can be employed to assess perceived burden, acceptance, and willingness to engage under varying interaction schemes. Advanced analysis methods, including fuzzy logic and multi-criteria decision-making (e.g., AHP, TOPSIS), can synthesize these diverse inputs into composite indices of user acceptance, engagement, and scalability potential. Importantly, privacy-preserving mechanisms must be clearly communicated to users, and their impact quantitatively evaluated, such as through pre- and post-implementation comparisons of participation rates, to determine how trust, consent transparency, and data protection influence user behavior. In this context, various consent-awareness strategies should be experimentally evaluated to quantify how transparency in privacy protection affects user attraction and the volume of collected data. Likewise, the influence of different incentive schemes and their adaptive deployment should be measured by analyzing system logs for variations in data volume and quality. Together, these assessments can provide deeper insights into the behavioral and technical dynamics of user participation, ultimately guiding the design of scalable, trustworthy, and user-friendly crowd-powered IPS.
4. Integrating MCS with Fog Computing for IPS: An emerging direction is the integration of MCS with fog computing to enhance IPS performance. By processing data at proximate network nodes such as access points or routers, fog computing can significantly reduce localization latency and improve context-awareness through localized inference. When combined with the scalability and adaptability of MCS, this layered architecture distributes computation efficiently, enhances resilience in large deployments, and supports high-precision, real-time positioning. Exploring such synergies could help future IPS deployments meet both precision and scalability demands.
5. New Modalities and Modal Synergies: Beyond current sensor modalities, breakthrough improvements may come from exploiting emerging technologies in sensing and communication in the crowd context. One promising example is the integration of wearable and ambient IoT sensors into the crowdsourcing framework. As wearable devices, such as smartwatches and fitness trackers, become increasingly ubiq-

uitous, they offer a valuable opportunity to augment smartphones by providing complementary sensor data. For instance, smartwatches can contribute fine-grained motion and activity context at significantly lower power consumption levels, often operating for up to a week on a single charge, thereby enabling sustained and energy-efficient data collection for crowd-powered IPS. Similarly, the growing deployment of smart building infrastructure (like smart lighting or sound sensors) could be tapped opportunistically by crowd IPS systems (with building consent) to enhance localization without dedicated hardware. *A visionary scenario could be an "ambient crowd-sensing" network: users' personal devices and the environment's sensors cooperate seamlessly, orchestrated by the IPS platform. This would blur the line between crowd-sourced data and infrastructure-based data, unlocking new levels of accuracy and resilience (since multiple data sources back each other up).* This approach also contributes to scalability and robustness – the system would be less brittle, as it's not tied to one signal type or device. Overall, pushing the envelope with new sensing modalities, and doing so in a crowd-collaborative way, stands to redefine what is achievable with IPS technology.

6. Quantum-Resilient Privacy and Cryptographic Frameworks: As quantum computing advances, existing encryption schemes may become vulnerable. Future IPS must therefore consider quantum-resilient privacy frameworks, especially for crowd-powered models involving sensitive user data. Research into post-quantum cryptography, such as lattice-based or hash-based schemes, should be incorporated early into privacy-by-design strategies for large-scale IPS. This is particularly critical in scenarios where user trust is paramount (e.g., healthcare facilities) and where long-term data confidentiality must be preserved even under future adversarial capabilities.
7. Self-Evolving Systems and Lifelong Learning in IPS: One of the most transformative breakthroughs in the future of crowd-powered IPS is the development of self-evolving systems, platforms capable of continual learning and dynamic adaptation over time without requiring explicit reprogramming. Unlike conventional systems that rely on static models or pre-trained datasets, lifelong learning-enabled IPS would continuously integrate new crowd-sourced observations, refine their internal representations of indoor environments, and autonomously adapt to changes such as environmental drift, evolving user behavior, or infrastructure modifications. These systems would not only scale with the user base but also evolve alongside it, ensuring long-term robustness and contextual relevance. Realizing this vision demands advancements in unsupervised and self-supervised learning, interpretable models, and autonomous performance monitoring techniques capable of detecting concept drift or degradation in data quality. Importantly, such self-evolving systems could also reduce the burden on users to frequently contribute through active participation. By compensating for reduced user input through continuous self-improvement and error correction, these systems can maintain data reliability and positioning accuracy. Moreover, the incorporation of trusted self-attestation mechanisms would help detect and mitigate issues such as fake participation or low-quality contributions, ensuring data integrity even under reduced user supervision. This breakthrough represents a shift toward more autonomous, resilient, and user-friendly IPS ecosystems.

8. Conclusion

Crowd-powered Indoor Positioning Systems (IPS) present a promising avenue for cost-efficient, scalable indoor localization, yet their widespread adoption hinges on addressing critical user-centric challenges. In this survey, we systematically examined the key user-centric challenges associated with crowd-powered IPS, including user participation schemes, incentive mechanisms, privacy and security risks, and the impact of data collection and localization on user devices. We mapped these issues across the architectural layers of crowd-powered IPS. Then, we analyzed existing studies on active, passive, and opportunistic participation, examining the nature of tasks assigned to users, their associated burden, and the objectives behind them. We also evaluated their impact on user-friendliness, reliability, and scalability. Additionally, we discussed the trade-offs inherent in different engagement schemes. Subsequently, we reviewed the limitations of existing incentive mechanisms after providing an overview of the differences between incentives in IPS and other crowd-driven fields, as well as discussing intrinsic and extrinsic motivations and the specific objectives of incentive mechanisms in IPS. Privacy and security concerns were further critically surveyed and assessed. Furthermore, we discussed the adverse effects of data collection and localization on user devices, emphasizing the need for energy-efficient strategies and intelligent resource management. Our findings reveal that these challenges are deeply interconnected, necessitating a holistic approach to ensure scalability, data reliability, and user engagement. Building on this, we proposed a roadmap for developing user-friendly, sustainable, and scalable IPS, emphasizing hybrid participation models that respect user time, accommodate diverse user preferences, and consider variations in motivations based on demographics, geography, and age. Furthermore, we advocated for AI-driven engagement techniques to generate time-, user-, environment-, and context-aware prompts, ensuring unobtrusive yet effective user participation while enhancing system reliability. We also recommended communicating value and purpose for fostering intrinsic motivation and societal impact and aligning incentive types with IPS objectives and user preferences when designing future adaptive incentive mechanisms to ensure cost-effectiveness and scalability. We also advocated for privacy-preserving frameworks that enhance robustness through explainable AI and adaptive defense mechanisms. Finally, we recommended practical strategies to mitigate the impact of data collection and localization processes on user devices to ensure user adoption and long-term engagement with these approaches. It is important to acknowledge that the long-term effectiveness of crowd-powered IPS, especially those driven by MCS campaigns, is inherently tied to sustained user engagement. Insufficient participation can render such systems ineffective, regardless of their technical sophistication. Addressing this limitation requires future research to focus not only on recruitment but also on strategies for maintaining participation over extended periods, balancing user effort, privacy, and incentive design. Moving forward, future research should prioritize the seamless integration of these strategies, ensuring that crowd-powered IPS can achieve widespread adoption while maintaining high accuracy, security, and usability in real-world applications.

CRediT authorship contribution statement

Ahmed Mansour: Writing – review & editing, Writing – original draft, Visualization, Methodology, Formal analysis, Conceptualization; **Wu Chen:** Supervision; **Eslam Ali:** Writing – review & editing; **Jingxian Wang:** Writing – review & editing; **Duojie Weng:** Writing – review & editing, Validation.

Data availability

No data was used for the research described in the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] L. Vaccari, A.M. Coruzzolo, F. Lolli, M.A. Sellitto, Indoor positioning systems in logistics: a review, Logistics 8 (4) (2024). https://doi.org/10.3390/logistics8040126
[2] CitiesABC, The ins and outs of indoor positioning systems: how they work, 2023. Accessed: January 2025. https://www.citiesabc.com/resources/the-ins-and-outs-of-indoor-positioning-systems-how-they-work/.

[3] Navigine, Industrial indoor positioning and tracking system for manufacturing, 2023. Accessed: January 2025. https://navigine.com/industries/manufacturing/.

[4] G.V. Research, Indoor Positioning and navigation market size, share, & trends analysis, 2023. Accessed: January 2025. https://www.grandviewresearch.com/industry-analysis/indoor-positioning-navigation-market-report.

[5] I. Battarra, R. Accorsi, R. Manzini, D. Dardari, A framework to design a scalable and reliable indoor positioning system-IPS for industrial applications, in: Warehousing and Material Handling Systems for the Digital Industry, Springer, 2024, pp. 473–503. https://doi.org/10.1007/978-3-031-50273-6_17

[6] M.M. Research, Indoor positioning and indoor navigation market - global industry, 2023. Accessed: January 2025. https://www.maximizemarketresearch.com/market-report/global-indoor-positioning-and-indoor-navigation-market/25418/.

[7] R. Want, Keynote Speech 1 – IPIN 2024, 2024, (https://ipin-conference.org/2024/keynote_speech_4/). Accessed: 2025-01-18.

[8] A. Mansour, J. Ye, Y. Li, H. Luo, J. Wang, D. Weng, W. Chen, Everywhere: a framework for ubiquitous indoor localization, IEEE Internet Things J. 10 (6) (2023) 5095–5113. https://doi.org/10.1109/JIOT.2022.3222003

[9] J. Wang, X. Mi, W. Chen, H. Luo, A. Mansour, Y. Li, Y. Yu, D. Weng, Tightly coupled bluetooth enhanced GNSS/PDR system for pedestrian navigation in dense urban environments, IEEE Trans. Instrum. Meas. 73 (2024) 1–13. https://doi.org/10.1109/TIM.2024.3481547

[10] S. Qiu, Z. Wang, H. Zhao, K. Qin, Z. Li, H. Hu, Inertial/magnetic sensors based pedestrian dead reckoning by means of multi-sensor fusion, Inf. Fusion 39 (2018) 108–119. https://doi.org/10.1016/j.inffus.2017.04.006

[11] J. Surowiecki, The Wisdom of Crowds, Anchor Books, Anchor Books, 2005. https://books.google.com.hk/books?id=Jrhsf5WlBxMC.

[12] P. Morales-Álvarez, P. Ruiz, R. Santos-Rodríguez, R. Molina, A.K. Katsaggelos, Scalable and efficient learning from crowds with Gaussian processes, Inf. Fusion 52 (2019) 110–127. https://doi.org/10.1016/j.inffus.2018.12.008

[13] J. Howe, The rise of crowdsourcing, Wired Mag. 14 (6) (2006) 1–4. https://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Aredes-sociais/Howe_The_Rise_of_Crowdsourcing.pdf.

[14] J.A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M.B. Srivastava, Participatory sensing, 2006. https://escholarship.org/content/qt19h777qd/qt19h777qd_noSplash_2d493afaeeef42e302645790cc924d1a.pdf.

[15] N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A.T. Campbell, A survey of mobile phone sensing, IEEE Commun. Mag. 48 (9) (2010) 140–150. https://doi.org/10.1109/MCOM.2010.5560598

[16] R.K. Ganti, F. Ye, H. Lei, Mobile crowdsensing: current state and future challenges, IEEE Commun. Mag. 49 (11) (2011) 32–39. https://doi.org/10.1109/MCOM.2011.6069707

[17] B. Guo, Z. Wang, Z. Yu, Y. Wang, N.Y. Yen, R. Huang, X. Zhou, Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm, ACM Comput. Surv. 48 (1) (2015). https://doi.org/10.1145/2794400

[18] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, P. Bouvry, A survey on mobile crowdsensing systems: challenges, solutions, and opportunities, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2419–2465. https://doi.org/10.1109/COMST.2019.2914030

[19] D. Cicek, B. Kantarci, Use of mobile crowdsensing in disaster management: a systematic review, challenges, and open issues, Sensors 23 (3) (2023). https://doi.org/10.3390/s23031699

[20] E. Zhang, R. Trujillo, J.M. Templeton, C. Poellabauer, A study on mobile crowd sensing systems for healthcare scenarios, IEEE Access 11 (2023) 140325–140347.

[21] L. Xiao, T. Chen, C. Xie, H. Dai, H.V. Poor, Mobile crowdsensing games in vehicular networks, IEEE Trans. Veh. Technol. 67 (2) (2017) 1535–1545.

[22] Y. Liu, L. Kong, G. Chen, Data-Oriented Mobile Crowdsensing: A Comprehensive Survey, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2849–2885. https://doi.org/10.1109/COMST.2019.2910855

[23] D. Suhag, V. Jha, A comprehensive survey on mobile crowdsensing systems, J. Syst. Archit. 142 (2023) 102952. https://doi.org/10.1016/j.sysarc.2023.102952

[24] V.S. Dasari, B. Kantarci, M. Pouryazdan, L. Foschini, M. Girolami, Game theory in mobile CrowdSensing: a comprehensive survey, Sensors 20 (7) (2020). https://doi.org/10.3390/s20072055

[25] S. Gisdakis, T. Giannetsos, P. Papadimitratos, Security, privacy, and incentive provision for mobile crowd sensing systems, IEEE Internet Things J. 3 (5) (2016) 839–853.

[26] S. Zhao, et al., A survey of sparse mobile crowdsensing: Developments and opportunities, IEEE Open Journal of the computer society. 3 (2022) 73–85. https://doi.org/10.1109/OJCS.2022.3177290

[27] Z. Wang, X. Pang, J. Hu, W. Liu, Q. Wang, Y. Li, H. Chen, When mobile crowdsensing meets privacy, IEEE Commun. Mag. 57 (9) (2019) 72–78.

[28] Y. Liu, Mobile Crowdsensing: issues and challenges, Encycl. Wirel. Netw. (2020) 861–865. https://link.springer.com/content/pdf/10.1007/978-3-319-78262-1_339.pdf.

[29] B. Lashkari, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, Crowdsourcing and sensing for indoor localization in IoT: A Review, IEEE Sens. J. 19 (7) (2019) 2408–2434. https://doi.org/10.1109/JSEN.2018.2880180

[30] L. Pei, M. Zhang, D. Zou, R. Chen, Y. Chen, A survey of crowd sensing opportunistic signals for indoor localization, Mob. Inf. Syst. 2016 (1) (2016) 4041291. https://doi.org/10.1155/2016/4041291.

[31] X. Zhou, T. Chen, D. Guo, X. Teng, B. Yuan, From one to crowd: a survey on crowdsourcing-based wireless indoor localization, Front. Comput. Sci. 12 (2018) 423–450. https://link.springer.com/article/10.1007/s11704-017-6520-z.

[32] B. Wang, Q. Chen, L.T. Yang, H.-C. Chao, Indoor smartphone localization via fingerprint crowdsourcing: challenges and approaches, IEEE Wirel. Commun. 23 (3) (2016) 82–89. https://doi.org/10.1109/MWC.2016.7498078

[33] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, X. Mao, Incentives for mobile crowd sensing: a survey, IEEE Commun. Surv. Tutor. 18 (1) (2016) 54–67. https://doi.org/10.1109/COMST.2015.2415528

[34] F. Restuccia, N. Ghosh, S. Bhattacharjee, S.K. Das, T. Melodia, Quality of information in mobile crowdsensing: survey and research challenges, ACM Trans. Sen. Netw. 13 (4) (2017). https://doi.org/10.1145/3139256

[35] A. Mansour, W. Chen, SUNS: a user-friendly scheme for seamless and ubiquitous navigation based on an enhanced indoor-outdoor environmental awareness approach, Remote Sens. 14 (20) (2022). https://doi.org/10.3390/rs14205263

[36] Y. Cheng, J. Ma, Z. Liu, Y. Wu, K. Wei, C. Dong, A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks, IEEE Trans. Dependable Secure Comput. 20 (3) (2023) 1771–1788. https://doi.org/10.1109/TDSC.2022.3163752

[37] Y. Cheng, J. Ma, Z. Liu, Z. Li, Y. Wu, C. Dong, R. Li, A privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing, IEEE Trans. Dependable Secure Comput. 20 (6) (2023) 5293–5311. https://doi.org/10.1109/TDSC.2023.3276976

[38] J. Krumm, A survey of computational location privacy, Pers. Ubiquitous Comput. 13 (6) (2009) 391–399. https://link.springer.com/article/10.1007/s00779-008-0212-5.

[39] J. Wang, Y. Wang, D. Zhang, S. Helal, Energy saving techniques in mobile crowd sensing: current state and future opportunities, IEEE Commun. Mag. 56 (5) (2018) 164–169. https://doi.org/10.1109/MCOM.2018.1700644

[40] S. Ramírez-Gallego, B. Krawczyk, S. García, M. Woźniak, F. Herrera, A survey on data preprocessing for data stream mining: current status and future directions, Neurocomputing 239 (2017) 39–57. https://doi.org/10.1016/j.neucom.2017.01.078

[41] A. Mansour, W. Chen, D. Weng, Y. Yang, J. Wang, Leveraging human mobility and pervasive smartphone measurements-based crowdsourcing for developing self-deployable and ubiquitous indoor positioning systems, Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci. 48 (2023) 1119–1125. https://doi.org/10.5194/isprs-archives-XLVIII-1-W2-2023-1119-2023

[42] M. Mallik, A.K. Panja, C. Chowdhury, Paving the way with machine learning for seamless indoor–outdoor positioning: a survey, Inf. Fusion 94 (2023) 126–151. https://doi.org/10.1016/j.inffus.2023.01.023

[43] B. Jang, H. Kim, J.w. Kim, Survey of landmark-based indoor positioning technologies, Inf. Fusion 89 (2023) 166–188. https://doi.org/10.1016/j.inffus.2022.08.013

[44] E.S. Lohan, J. Torres-Sospedra, H. Leppäkoski, P. Richter, Z. Peng, J. Huerta, Wi-Fi crowdsourced fingerprinting dataset for indoor positioning, Data 2 (4) (2017). https://doi.org/10.3390/data2040032

[45] Y. Guo, W. Wang, X. Chen, FreeNavi: landmark-based mapless indoor navigation based on WiFi fingerprints, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), 2017, pp. 1–5. https://doi.org/10.1109/VTCSpring.2017.8108350

[46] Y.J. Li, K.F. Xu, J.J. Shao, K.K. Chi, Maintenance of Wi-Fi fingerprint database by crowdsourcing for indoor localization, 2015. https://doi.org/10.1007/978-3-662-46981-1_58

[47] W.W. Li, Z. Su, R.D. Li, K. Zhang, Q.C. Xu, Abnormal crowd traffic detection for crowdsourced indoor positioning in heterogeneous communications networks, IEEE Trans. Netw. Sci. Eng. 7 (4) (2020) 2494–2505. https://doi.org/10.1109/TNSE.2020.3014380

[48] Y.Y. Wei, R. Zheng, Efficient Wi-Fi fingerprint crowdsourcing for indoor localization, IEEE Sens. J. 22 (6) (2022) 5055–5062. https://doi.org/10.1109/JSEN.2021.3087954

[49] R. Santos, R. Leonardo, M. Barandas, D. Moreira, T. Rocha, P. Alves, J.P. Oliveira, H. Gamboa, Crowdsourcing-based fingerprinting for indoor location in multi-storey buildings, IEEE Access 9 (2021) 31143–31160. https://doi.org/10.1109/ACCESS.2021.3060123

[50] V. Radu, M.K. Marina, HiMLoc: indoor smartphone localization via activity aware pedestrian dead reckoning with selective crowdsourced WiFi fingerprinting, in: International Conference on Indoor Positioning and Indoor Navigation, 2013, pp. 1–10. https://doi.org/10.1109/IPIN.2013.6817916

[51] Y.C. He, X. Zhang, Vision-aided self-calibration of a wireless propagation model for crowdsourcing-based indoor localization, Measurement 205 (2022). https://doi.org/10.1016/j.measurement.2022.112183

[52] H. Xu, Z. Yang, Z. Zhou, L. Shangguan, K. Yi, Y. Liu, Enhancing wifi-based localization with visual clues, in: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 963–974. https://doi.org/10.1145/2750858.2807516

[53] T. Liu, X. Zhang, Q.Q. Li, Z.X. Fang, N. Tahir, An accurate visual-inertial integrated geo-tagging method for crowdsourcing-based indoor localization, Remote Sens. 11 (16) (2019). https://doi.org/10.3390/rs11161912

[54] A. Mahmoud, M.G. Mohamed, A. El Shazly, Low-cost framework for 3D reconstruction and track detection of the railway network using video data, Egypt. J. Remote Sens. Space Sci. 25 (4) (2022) 1001–1012. https://doi.org/10.1016/j.ejrs.2022.11.001

[55] M. Adham, W. Chen, Y. LI, T. Liu, Towards Robust Global VINS: Innovative SemanticAware and multi-level geometric constraints approach for dynamic feature filtering in urban environments, IEEE Trans. Intell. Vehicles (2024) 1–24. https://doi.org/10.1109/TIV.2024.3487593

[56] J. Dong, M. Noreikis, Y. Xiao, A. Ylä-Jääski, ViNav: a vision-based indoor navigation system for smartphones, IEEE Trans. Mob. Comput. 18 (6) (2019) 1461–1475. https://doi.org/10.1109/TMC.2018.2857772

[57] F. Gu, J.W. Niu, L.J. Duan, WAIPO: a fusion-based collaborative indoor localization system on smartphones, IEEE-ACM Trans. Netw. 25 (4) (2017) 2267–2280. https:

//doi.org/10.1109/TNET.2017.2680448
[58] X. Zhang, T. Liu, Q. Li, Z. Fang, Crowdsourcing trajectory based indoor positioning multisource database construction on smartphones, in: S. Di Martino, Z. Fang, K.-J. Li (Eds.), Web and Wireless Geographical Information Systems, Springer International Publishing, Cham, 2020, pp. 145–155.
[59] J. Dong, Y. Xiao, M. Noreikis, Z. Ou, A. Ylä-Jääski, Demo: iMoon: using smartphones for image-based indoor navigation, in: Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, SenSys '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 449–450. https://doi.org/10.1145/2809695.2817848
[60] E. Shahid, Q. Arain, S. Kumari, I. Farah, Images based indoor positioning using AI and crowdsourcing, in: Proceedings of the 2019 8th International Conference on Educational and Information Technology, ICEIT 2019, Association for Computing Machinery, New York, NY, USA, 2019, p. 97–101. https://doi.org/10.1145/3318396.3318415
[61] E. Shahid, Q.A. Arain, Indoor positioning: an image-based crowdsource machine learning approach, Multimed. Tools Appl. 80 (17) (2021) 26213–26235. https://doi.org/10.1007/s11042-021-10906-z
[62] M.X. Tang, Y.C. Zhao, Q.X. Ma, J.S. Hao, B. Chen, CrowdLoc: robust image indoor localization with edge-assisted crowdsensing, J. Syst. Archit. 131 (2022). https://doi.org/10.1016/j.sysarc.2022.102732
[63] V. Upadhyay, M. Balakrishnan, Monocular localization using invariant image feature matching to assist navigation, in: Computers Helping People with Special Needs, Springer International Publishing, Cham, 2022, pp. 178–186. https://doi.org/10.1007/978-3-031-08648-9_21
[64] X.G. Niu, Z.J. Zhang, A.K. Wang, J.B. Liu, S.B. Liu, Online learning-based wifi radio map updating considering high-dynamic environmental factors, IEEE Access 7 (2019) 110074–110085. https://doi.org/10.1109/ACCESS.2019.2933583
[65] Q. Wan, X.Q. Duan, Y. Yu, R.Z. Chen, L. Chen, Self-calibrated multi-floor localization based on Wi-Fi ranging/crowdsourced fingerprinting and low-cost sensors, Remote Sens. 14 (21) (2022). https://doi.org/10.3390/rs14215376
[66] AIMultiple, Crowdsourcing: Benefits and Challenges, 2021, (AIMultiple). https://research.aimultiple.com/crowdsourcing/.
[67] R. Liang, Z. Ye, J. Zhang, L. Shi, Z. Shen, W. Du, Continued participation in crowdsourcing innovation: the role of web-specific computer self-efficacy, IEEE Access 11 (2023) 100309–100322. https://doi.org/10.1109/ACCESS.2023.3314331
[68] M. Hossain, I. Kauranen, Crowdsourcing: a comprehensive literature review, Strategic Outsourcing Int. J. 8 (1) (2015) 2–22. https://doi.org/10.1108/SO-12-2014-0029
[69] A. Alshami, M. Elsayed, E. Ali, A.E.E. Eltoukhy, T. Zayed, Harnessing the power of ChatGPT for automating systematic review process: methodology, case study, limitations, and future directions, Systems 11 (7) (2023). https://doi.org/10.3390/systems11070351
[70] M. Hossain, Crowdsourcing: Activities, incentives and users' motivations to participate, in: 2012 International Conference on Innovation Management and Technology Research, 2012, pp. 501–506. https://doi.org/10.1109/ICIMTR.2012.6236447
[71] J. Lu, W. Li, Q. Wang, Y. Zhang, Research on data quality control of crowdsourcing annotation: a survey, in: 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2020, pp. 201–208. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00044
[72] A. Katmada, A. Satsiou, I. Kompatsiaris, Incentive mechanisms for crowdsourcing platforms, in: Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12–14, 2016, Proceedings 3, Springer, 2016, pp. 3–18. https://doi.org/10.1007/978-3-319-45982-0_1
[73] M. Lee, S.H. Jung, S. Lee, D. Han, Elekspot: a Platform for Urban Place Recognition via Crowdsourcing, in: 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, 2012, pp. 190–195. https://doi.org/10.1109/SAINT.2012.35
[74] J. Ahn, D. Han, Crowd-assisted radio map construction for Wi-Fi positioning systems, in: 2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2017, pp. 1–8. https://doi.org/10.1109/IPIN.2017.8115872
[75] X. Zhou, J. Wei, F. Zhao, H. Luo, L. Ye, A shop-level location algorithm based on CNN for crowdsourcing fingerprint, in: 2018 Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS), 2018, pp. 1–7. https://doi.org/10.1109/UPINLBS.2018.8559873
[76] D. Han, B. Moon, G. Yoon, Address-based crowdsourcing radio map construction for Wi-Fi positioning systems, in: 2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2014, pp. 58–67. https://doi.org/10.1109/IPIN.2014.7275468
[77] Z. Li, X. Zhao, F. Hu, Z. Zhao, J.L. Carrera Villacrés, T. Braun, SoiCP: a seamless outdoor–indoor crowdsensing positioning system, IEEE Internet Things J. 6 (5) (2019) 8626–8644. https://doi.org/10.1109/JIOT.2019.2921561
[78] Y. Du, F. Sailhan, V. Issarny, Let opportunistic crowdsensors work together for resource-efficient, quality-aware observations, in: 2020 IEEE International Conference on Pervasive Computing and Communications (PerCom), 2020, pp. 1–10. https://doi.org/10.1109/PerCom45495.2020.9127391
[79] A. Trifan, M. Oliveira, J.L. Oliveira, Passive sensing of health outcomes through smartphones: systematic review of current solutions and possible limitations, JMIR Mhealth Uhealth 7 (8) (2019) e12649. https://doi.org/10.2196/12649
[80] H. Alhazmi, A. Imran, M.A. Alsheikh, Perception of digital privacy protection: an empirical study using gdpr framework, 2024. 2411.12223
[81] H. Xia, B. McKernan, Privacy in crowdsourcing: a review of the threats and challenges, Comput. Supported Cooperative Work (CSCW) 29 (2020) 263–301. https://doi.org/10.1007/s10606-020-09374-0
[82] S. Kumar, M. Faisal, Exploring the issues and challenges in crowdsourcing: an empirical investigation, in: International Conference on Information Systems and Management Science, Springer, 2023, pp. 531–544. https://doi.org/10.1007/978-3-031-66410-6_42
[83] Y. Gu, C.F. Zhou, A. Wieser, Z.M. Zhou, Trajectory estimation and crowdsourced radio map establishment from foot-mounted IMUs, Wi-Fi fingerprints, and GPS positions, IEEE Sens. J. 19 (3) (2019) 1104–1113. https://doi.org/10.1109/JSEN.2018.2877804
[84] E. Ciceri, Humans in the loop: optimization of active and passive crowdsourcing, 2015. https://hdl.handle.net/10589/102903.
[85] M.V. Velázquez, A. Faka, O. Kounadi, Chapter 19 - Crowdsourcing applications for monitoring the urban environment, in: G.P. Petropoulos, C. Chalkias (Eds.), Geographical Information Science, Elsevier, 2024, pp. 397–413. https://doi.org/10.1016/B978-0-443-13605-4.00015-1
[86] B. Mozafari, P. Sarkar, M. Franklin, M. Jordan, S. Madden, Scaling up crowdsourcing to very large datasets: a case for active learning, Proc. VLDB Endow. 8 (2) (2014) 125–136. https://doi.org/10.14778/2735471.2735474
[87] Y. Li, L. Chang, L. Li, X. Bao, T. Gu, Key research issues and related technologies in crowdsourcing data collection, Wirel. Commun. Mob. Comput. 2021 (1) (2021) 8745897. https://doi.org/10.1155/2021/8745897
[88] Y. Fang, H. Sun, P. Chen, J. Huai, On the cost complexity of crowdsourcing, in: IJCAI, 2018, pp. 1531–1537. https://www.ijcai.org/Proceedings/2018/0212. pdf.
[89] L. Hao, C. Jin, X. Gao, F. Wu, G. Chen, Towards cost-effective and budget-balanced task allocation in crowdsourcing systems, in: 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), 2017, pp. 1–8. https://doi.org/10.1109/PCCC.2017.8280461
[90] A. Gruenheid, D. Kossmann, Cost and quality trade-offs in crowdsourcing, DBCrowd 1025 (2013) 43–46. https://ceur-ws.org/Vol-1025/vision2.pdf.
[91] A. Alkharashi, K. Renaud, Privacy in crowdsourcing: a systematic review, in: Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21, Springer, 2018, pp. 387–400. https://doi.org/10.1007/978-3-319-99136-8_21
[92] A. Koschmider, M. Schaarschmidt, A Crowdsourcing-based learning approach to activate active learning, 2017. https://dl.gi.de/handle/20.500.12116/4882.
[93] D. Yang, G. Xue, X. Fang, J. Tang, Incentive mechanisms for crowdsensing: crowdsourcing with smartphones, IEEE/ACM Trans. Netw. 24 (3) (2016) 1732–1744. https://doi.org/10.1109/TNET.2015.2421897
[94] D. Yang, G. Xue, X. Fang, J. Tang, Incentive mechanisms for crowdsensing: crowdsourcing with smartphones, IEEE/ACM Trans. Netw. 24 (3) (2016) 1732–1744. https://doi.org/10.1109/TNET.2015.2421897
[95] L. Wang, Y. Yang, Y. Wang, Do higher incentives lead to better performance? - An exploratory study on software crowdsourcing, in: 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2019, pp. 1–11. https://doi.org/10.1109/ESEM.2019.8870175
[96] Y.T. Wen, J.Y. Shi, Q. Zhang, X.H. Tian, Z.Y. Huang, H. Yu, Y. Cheng, X.M. Shen, Quality-driven auction-based incentive mechanism for mobile crowd sensing, IEEE Trans. Veh. Technol. 64 (9) (2015) 4203–4214. https://doi.org/10.1109/TVT.2014.2363842
[97] H. Gao, H. Xu, L. Li, C. Zhou, H. Zhai, Y. Chen, Z. Han, Mean-field-game-based dynamic task pricing in mobile crowdsensing, IEEE Internet Things J. 9 (18) (2022) 18098–18112. https://doi.org/10.1109/JIOT.2022.3161952
[98] N.V.-Q. Truong, L.C. Dinh, S. Stein, L. Tran-Thanh, N.R. Jennings, Efficient and adaptive incentive selection for crowdsourcing contests, Appl. Intell. 53 (8) (2023) 9204–9234. https://doi.org/10.1007/s10489-022-03593-2
[99] R.I. Ogie, Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: from literature review to a conceptual framework, Human-centric Comput. Inf. Sci. 6 (1) (2016) 24. https://doi.org/10.1186/s13673-016-0080-3
[100] X. Zhang, G. Xue, R. Yu, D. Yang, J. Tang, Truthful incentive mechanisms for crowdsourcing, in: Proc. IEEE INFOCOM, 2015, pp. 2830–2838. https://doi.org/10.1109/INFOCOM.2015.7218654
[101] E.N. Moghaddam, A. Aliahmadi, M. Bagherzadeh, S. Markovic, M. Micevski, F. Saghafi, Let me choose what I want: The influence of incentive choice flexibility on the quality of crowdsourcing solutions to innovation problems, Technovation 120 (2023) 102679. https://doi.org/10.1016/j.technovation.2022.102679
[102] Y. Zhan, Y. Xia, J. Zhang, T. Li, Y. Wang, An incentive mechanism design for mobile crowdsensing with demand uncertainties, Inf. Sci. 528 (2020) 1–16. https://doi.org/10.1016/j.ins.2020.03.109
[103] E. Wu, Z. Peng, Research Progress on Incentive Mechanisms in Mobile Crowdsensing, IEEE Internet Things J. 11 (14) (2024) 24621–24633. https://doi.org/10.1109/JIOT.2024.3400965
[104] Y. Fu, D. Liang, Z. Xu, W. Duan, Exploiting game equilibrium mechanisms towards social trust-based group consensus reaching, Inf. Fusion 112 (2024) 102558. https://doi.org/10.1016/j.inffus.2024.102558
[105] M. Tang, H. Liao, X. Wu, A Stackelberg game model for large-scale group decision making based on cooperative incentives, Inf. Fusion 96 (2023) 103–116. https://doi.org/10.1016/j.inffus.2023.03.013
[106] T.H. Rafi, F.A. Noor, T. Hussain, D.-K. Chae, Fairness and privacy preserving in federated learning: a survey, Inf. Fusion 105 (2024) 102198. https://doi.org/10.1016/j.inffus.2023.102198
[107] R. Gonen, E. Pavlov, An incentive-compatible multi-armed bandit mechanism, in: Proceedings of the Twenty-Sixth Annual ACM Symposium on Principles of Distributed Computing, PODC '07, Association for Computing Machinery, New York, NY, USA, 2007, p. 362–363. https://doi.org/10.1145/1281100.1281174
[108] N.V.-Q. Truong, L.C. Dinh, S. Stein, L. Tran-Thanh, N.R. Jennings, Efficient and adaptive incentive selection for crowdsourcing contests, Appl. Intell. 53 (8) (2023)

9204–9234. https://doi.org/10.1007/s10489-022-03593-2
[109] X. Zhang, G. Xue, R. Yu, D. Yang, J. Tang, Truthful incentive mechanisms for crowdsourcing, in: 2015 IEEE Conference on Computer Communications (INFOCOM), IEEE, 2015, pp. 2830–2838.
[110] Y. Chris Zhao, Q. Zhu, Effects of extrinsic and intrinsic motivation on participation in crowdsourcing contest: a perspective of self-determination theory, Online Inf. Rev. 38 (7) (2014) 896–917. https://doi.org/10.1108/OIR-08-2014-0188
[111] T.O. Tokosi, B.M. Scholtz, A classification framework of mobile health crowdsensing research: a scoping review, in: Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019, SAICSIT '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–12. https://doi.org/10.1145/3351108.3351113
[112] S.N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, A. Bani-Hani, Blockchain smart contracts: applications, challenges, and future trends, Peer-to-peer Netw. Appl. 14 (2021) 2901–2925. https://doi.org/10.1007/s12083-021-01127-0
[113] S. Kivilo, Designing a Token Economy: Incentives, Governance, and Tokenomics, Master's thesis, Tallinn University of Technology, 2023. https://www.researchgate.net/profile/Sowelu-Avanzo-2/publication/390271393_Designing_a_Token_Economy_Incentives_Governance_and_Tokenomics/links/67e6abee95231d5ba59c3ba6/Designing-a-Token-Economy-Incentives-Governance-and-Tokenomics.pdf.
[114] A. Mansour, W. Chen, H. Luo, Y. Li, J. Wang, D. Weng, Drift control of pedestrian dead reckoning (PDR) for long period navigation under different smartphone poses, Eng. Proc. 10 (1) (2021). https://doi.org/10.3390/ecsa-8-11302
[115] H. Kressler, Motivate and Reward: Performance Appraisal and Incentive Systems for Business Success, Springer, 2003. https://doi.org/10.1057/9781403937711
[116] M. Kwak, C. Hamm, S. Park, T.T. Kwon, Magnetic field based indoor localization system: a crowdsourcing approach, in: 2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2019, pp. 1–8. https://doi.org/10.1109/IPIN.2019.8911795
[117] A.K.M. Mahtab Hossain, H. Nguyen Van, W.-S. Soh, Utilization of user feedback in indoor positioning system, Pervasive Mob. Comput. 6 (4) (2010) 467–481. Human Behavior in Ubiquitous Environments: Modeling of Human Mobility Patterns, https://doi.org/10.1016/j.pmcj.2010.04.003
[118] Z. Xu, B. Huang, B. Jia, G. Mao, Enhancing WiFi fingerprinting localization through a Co-teaching approach using crowdsourced sequential RSS and IMU data, IEEE Internet Things J. 11 (2) (2024) 3550–3562. https://doi.org/10.1109/JIOT.2023.3297521
[119] W. Cheng, Y. Zhang, E. Clay, Comprehensive performance assessment of passive crowdsourcing for counting pedestrians and bikes, 2022. https://doi.org/10.31979/mti.2022.2025
[120] R. Guan, R. Harle, Crowdsourcing mobile data for a passive indoor positioning system - the MAA case study, in: 2022 18th International Conference on Mobility, Sensing and Networking (MSN), 2022, pp. 59–67. https://doi.org/10.1109/MSN57253.2022.00024
[121] Y. Zhao, W.-C. Wong, T. Feng, H.K. Garg, Calibration-free indoor positioning using crowdsourced data and multidimensional scaling, IEEE Trans. Wirel. Commun. 19 (3) (2020) 1770–1785. https://doi.org/10.1109/TWC.2019.2957363
[122] Y. Zhang, L. Ma, Radio map crowdsourcing update method using sparse representation and low rank matrix recovery for WLAN indoor positioning system, IEEE Wirel. Commun. Lett. 10 (6) (2021) 1188–1191. https://doi.org/10.1109/LWC.2021.3061539
[123] S. Sorour, Y. Lostanlen, S. Valaee, Reduced-effort generation of indoor radio maps using crowdsourcing and manifold alignment, in: 6th International Symposium on Telecommunications (IST), 2012, pp. 354–358. https://doi.org/10.1109/ISTEL.2012.6483011
[124] Y. Dong, G. He, T. Arslan, Y. Yang, Y. Ma, Crowdsourced indoor positioning with scalable WiFi augmentation, Sensors 23 (8) (2023). https://doi.org/10.3390/s23084095
[125] F. Tian, B. Liu, X. Sun, X. Zhang, G. Cao, L. Gui, Movement-based incentive for crowdsourcing, IEEE Trans. Veh. Technol. 66 (8) (2017) 7223–7233. https://doi.org/10.1109/TVT.2017.2654355
[126] T. Yu, L. Gui, T. Yu, J. Wang, Walrasian equilibrium-based incentive scheme for mobile crowdsourcing fingerprint localization, Sensors 19 (12) (2019). https://doi.org/10.3390/s19122693
[127] L. Xie, T.H. Luan, Z. Su, Q. Xu, N. Chen, A game-theoretical approach for secure crowdsourcing-based indoor navigation system with reputation mechanism, IEEE Internet Things J. 9 (7) (2022) 5524–5536. https://doi.org/10.1109/JIOT.2021.3111999
[128] W. Li, C. Zhang, Z. Liu, Y. Tanaka, Incentive mechanism design for crowdsourcing-based indoor localization, IEEE ACCESS 6 (2018) 54042–54051. https://ieeexplore.ieee.org/ielx7/6287639/8274985/08457189.pdf?tp=&arnumber=8457189&isnumber=8274985&ref=. https://doi.org/10.1109/ACCESS.2018.2869202
[129] A. Mansour, Indoor Localization Based on Multi-Sensor Fusion, Crowdsourcing, and Multi-User Collaboration, Ph.D. thesis, Hong Kong Polytechnic University, 2023. https://theses.lib.polyu.edu.hk/handle/200/12441.
[130] T. Li, Y. Chen, R. Zhang, Y. Zhang, T. Hedgpeth, Secure crowdsourced indoor positioning systems, in: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, pp. 1034–1042. https://doi.org/10.1109/INFOCOM.2018.8486398
[131] L. Xiang, B. Li, B. Li, Privacy-preserving inference in crowdsourcing systems, in: 2017 IEEE Conference on Communications and Network Security (CNS), 2017, pp. 1–9. https://doi.org/10.1109/CNS.2017.8228623
[132] P.S. Farahsari, A. Farahzadi, J. Rezazadeh, A. Bagheri, A survey on indoor positioning systems for IoT-based applications, IEEE Internet Things J. 9 (10) (2022) 7680–7699. https://doi.org/10.1109/JIOT.2022.3149048
[133] X. Cui, P. Sun, N. Guo, Privacy protection in mobile crowdsensing based on local differential privacy, in: Proceedings of the 2024 14th International Conference on Communication and Network Security, ICCNS '24, Association for Computing Machinery, New York, NY, USA, 2025, p. 29–34. https://doi.org/10.1145/3711618.3711625
[134] J.W. Kim, K. Edemacu, B. Jang, Privacy-preserving mechanisms for location privacy in mobile crowdsensing: a survey, J. Netw. Comput. Appl. 200 (2022) 103315. https://www.sciencedirect.com/science/article/pii/S1084804521003039. https://doi.org/10.1016/j.jnca.2021.103315
[135] X. Han, X. Niu, L. Chen, S. Qin, Privacy protection strategies in mobile crowdsensing from the framework perspective, in: 2024 29th International Conference on Automation and Computing (ICAC), 2024, pp. 1–6. https://doi.org/10.1109/ICAC61394.2024.10718827
[136] K. Han, H. Liu, S. Tang, M. Xiao, J. Luo, Differentially private mechanisms for budget limited mobile crowdsourcing, IEEE Trans. Mob. Comput. 18 (4) (2019) 934–946. https://doi.org/10.1109/TMC.2018.2848265
[137] J. Wang, M. Li, Y. He, H. Li, K. Xiao, C. Wang, A blockchain based privacy-preserving incentive mechanism in crowdsensing applications, IEEE Access 6 (2018) 17545–17556. https://doi.org/10.1109/ACCESS.2018. 2805837
[138] B. Zhao, X. Liu, W.-N. Chen, R.H. Deng, CrowdFL: privacy-preserving mobile crowdsensing system via federated learning, IEEE Trans. Mob. Comput. 22 (8) (2023) 4607–4619. https://doi.org/10.1109/TMC.2022.3157603
[139] S. Feng, Y. Qin, Z. Zeng, B. Wen, W. Zhong, N. Wang, W. Guo, Y. Zhang, A paillier homomorphic encryption-based lightweight privacy protection model for mobile crowd sensing networks, Informatica 49 (7) (2025). https://doi.org/10.31449/inf.v49i7.6676
[140] C. Zhang, T. Wu, W. Zhang, Data privacy and cybersecurity in mobile crowdsensing, Electronics 14 (5) (2025). 1038 https://doi.org/10.3390/electronics14051038
[141] V. Agate, P. Ferraro, G. Lo Re, S.K. Das, BLIND: a privacy preserving truth discovery system for mobile crowdsensing, J. Netw. Comput. Appl. 223 (2024) 103811. https://www.sciencedirect.com/science/article/pii/S1084804523002308. https://doi.org/10.1016/j.jnca.2023.103811
[142] H. Chen, X. Mou, Z. Wang, T. Wu, X. Wang, C. Wang, R. Song, L. Song, X. Jiang, X. Zhang, Y. Li, Multi-functional homomorphic encryption method based on crowd sensing networks, IEEE Access 13 (2025) 36795–36803. https://doi.org/10.1109/ACCESS.2025.3544763
[143] H. Wu, L. Wang, G. Xue, J. Tang, D. Yang, Enabling data trustworthiness and user privacy in mobile crowdsensing, IEEE/ACM Trans. Netw. 27 (6) (2019) 2294–2307. https://doi.org/10.1109/TNET.2019.2944984
[144] J. Tang, S. Fu, X. Liu, Y. Luo, M. Xu, Achieving privacy-preserving and lightweight truth discovery in mobile crowdsensing, IEEE Trans. Knowl. Data Eng. 34 (11) (2022) 5140–5153. https://doi.org/10.1109/TKDE.2021.3054409
[145] K. Rabimba, L. Xu, L. Chen, F. Zhang, Z. Gao, W. Shi, Lessons learned from blockchain applications of trusted execution environments and implications for future research, in: Proceedings of the 10th International Workshop on Hardware and Architectural Support for Security and Privacy, HASP '21, Association for Computing Machinery, New York, NY, USA, 2022, p. 8. https://doi.org/10.1145/3505253.3505259
[146] Z. Zhang, D.H. Yum, M. Shin, PARS: privacy-aware reward system for mobile crowdsensing systems, Sensors 21 (21) (2021). https://doi.org/10.3390/s21217045
[147] S. Zou, J. Xi, H. Wang, G. Xu, CrowdBLPS: a blockchain-based location-privacy-preserving mobile crowdsensing system, IEEE Trans. Ind. Inf. 16 (6) (2020) 4206–4218. https://doi.org/10.1109/TII.2019.2957791
[148] S. Sodagari, Trends for mobile IoT crowdsourcing privacy and security in the big data era, IEEE Trans. Technol. Soc. 3 (3) (2022) 199–225. https://doi.org/10.1109/TTS.2022.3191515
[149] R. Wang, L. Gu, J. Li, J. Wang, J. Sun, W. Wan, GenRAN: GenFusion-guided Reversible Anonymization Network for face privacy preserving, Inf. Fusion 121 (2025) 103120. https://doi.org/10.1016/j.inffus.2025.103120
[150] P. Zhang, X. Fang, Z. Zhang, X. Fang, Y. Liu, J. Zhang, Horizontal multi-party data publishing via discriminator regularization and adaptive noise under differential privacy, Inf. Fusion 120 (2025) 103046. https://doi.org/10.1016/j.inffus.2025.103046
[151] C. Dwork, F. McSherry, K. Nissim, A. Smith, Calibrating noise to sensitivity in private data analysis, in: Theory of Cryptography Conference, Springer, 2006, pp. 265–284. https://doi.org/10.1007/11681878_14
[152] F. Peng, S. Tang, B. Zhao, Y. Liu, A privacy-preserving data aggregation of mobile crowdsensing based on local differential privacy, in: Proceedings of the ACM Turing Celebration Conference - China, ACM TURC '19, Association for Computing Machinery, New York, NY, USA, 2019, p. 5. https://doi.org/10.1145/3321408.3321602
[153] J. Chen, H. Ma, D. Zhao, L. Liu, Correlated differential privacy protection for mobile crowdsensing, IEEE Trans. Big Data 7 (4) (2021) 784–795. https://doi.org/10.1109/TBDATA.2017.2777862
[154] M. Guan, H. Bao, J. Wang, L. Xing, H.-N. Dai, PEFed: enhancing privacy and efficiency in federated learning via removable perturbation and decentralized encryption, Inf. Fusion 122 (2025) 103187. https://doi.org/10.1016/j.inffus.2025.103187
[155] C. Ying, H. Jin, X. Wang, Y. Luo, Double insurance: incentivized federated learning with differential privacy in mobile crowdsensing, in: 2020 International Symposium on Reliable Distributed Systems (SRDS), 2020, pp. 81–90. https://doi.org/10.1109/SRDS51746.2020.00016

[156] J. Wang, M.T. Quasim, B. Yi, Privacy-preserving heterogeneous multi-modal sensor data fusion via federated learning for smart healthcare, Inf. Fusion 120 (2025) 103084. https://www.sciencedirect.com/science/article/pii/S1566253525001575. https://doi.org/10.1016/j.inffus.2025.103084

[157] J. Guo, L. Su, J. Liu, J. Ding, X. Liu, B. Huang, L. Li, Auction-based client selection for online federated learning, Inf. Fusion 112 (2024) 102549. https://www.sciencedirect.com/science/article/pii/S1566253524003270. https://doi.org/10.1016/j.inffus.2024.102549

[158] Y. Zhan, J. Zhang, Z. Hong, L. Wu, P. Li, S. Guo, A survey of incentive mechanism design for federated learning, IEEE Trans. Emerg. Top. Comput. 10 (2) (2022) 1035–1044. https://doi.org/10.1109/TETC.2021.3063517

[159] Q. Mei, W. Guo, Y. Zhao, L. Nie, D. Adhikari, Blockchain-based privacy-preserving incentive scheme for internet of electric vehicle, Inf. Fusion 115 (2025) 102732. https://www.sciencedirect.com/science/article/pii/S1566253524005104. https://doi.org/10.1016/j.inffus.2024.102732

[160] B.S. Ciftler, A. Albaseer, N. Lasla, M. Abdallah, Federated learning for RSS fingerprint-based localization: a privacy-preserving crowdsourcing method, in: 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 2112–2117. https://doi.org/10.1109/IWCMC48107.2020.9148111

[161] W. Li, C. Zhang, Y. Tanaka, Pseudo label-driven federated learning-based decentralized indoor localization via mobile crowdsourcing, IEEE Sens. J. 20 (19) (2020) 11556–11565. https://ieeexplore.ieee.org/document/9103044/. https://doi.org/10.1109/JSEN.2020.2998116

[162] Y.X. Liu, H.C.W. Li, J. Xiao, H. Jin, Ieee, FLoc: fingerprint-based indoor localization system under a federated learning updating framework, 2019. https://doi.org/10.1109/MSN48538.2019.00033

[163] Z.S. Wu, X.P. Wu, X.L. Long, Y.L. Long, A Privacy-Preserved Online Personalized Federated Learning Framework for Indoor Localization, IEEE, 2021. https://ieeexplore.ieee.org/document/9658722/. https://doi.org/10.1109/SMC52423.2021.9658722

[164] H. Qi, J. Luo, Q. Li, J. Wu, A comparative trade-off analysis on accuracy and efficiency for federated learning in demand forecasting, Appl. Soft Comput. 182 (2025) 113561. https://www.sciencedirect.com/science/article/pii/S1568494625008725. https://doi.org/10.1016/j.asoc.2025.113561

[165] N.S. Joynab, M.N. Islam, R.R. Aliya, A.S.M.R. Hasan, N.I. Khan, I.H. Sarker, A federated learning aided system for classifying cervical cancer using PAP-SMEAR images, Inf. Med. Unlocked 47 (2024) 101496. https://www.sciencedirect.com/science/article/pii/S2352914824000522. https://doi.org/10.1016/j.imu.2024.101496

[166] P. Armengol, R. Tobkes, K. Akkaya, B.S. Ciftler, I. Guvenc, IEEE, Efficient privacy-preserving fingerprint-based indoor localization using crowdsourcing, 2015. Times Cited in Web of Science Core Collection: 7 Total Times Cited: 7 Cited Reference Count: 9. https://ieeexplore.ieee.org/document/7366991/. https://doi.org/10.1109/MASS.2015.76

[167] X. Ding, R. Lv, X. Pang, J. Hu, Z. Wang, X. Yang, X. Li, Privacy-preserving task allocation for edge computing-based mobile crowdsensing, Comput. Electr. Eng. 97 (2022) 107528. https://www.sciencedirect.com/science/article/pii/S0045790621004730?via%3Dihub. https://doi.org/10.1016/j.compeleceng.2021.107528

[168] X. Sun, H.J. Ai, J.J. Tao, T. Hu, Y.S. Cheng, BERT-ADLOC: a secure crowdsourced indoor localization system based on BLE fingerprints, Appl. Soft Comput. 104 (2021). https://www.sciencedirect.com/science/article/pii/S1568494621001605?via%3Dihub. https://doi.org/10.1016/j.asoc.2021.107237

[169] R. Zhang, Z. Li, N.N. Xiong, S. Zhang, A. Liu, TDTA: a truth detection based task assignment scheme for mobile crowdsourced Industrial Internet of Things, Inf. Sci. 610 (2022) 246–265. https://www.sciencedirect.com/science/article/pii/S0020025522008763. https://doi.org/10.1016/j.ins.2022.07.176

[170] I.. Conference, Keynote Speech 1 – IPIN 2024, 2024, (https://ipin-conference.org/2024/keynote_speech_1/). Accessed: 2025-01-18.

[171] A. Mansour, W. Chen, H. Luo, D. Weng, The power of many: multi-user collaborative indoor localization for boosting standalone user-based systems in different scenarios, in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023), 2023, pp. 3148–3161. https://doi.org/10.33012/2023.19439

[172] A. Mansour, W. Chen, Towards ubiquitous IPS: leveraging crowdsourced data accumulation over time to alleviate reliance on external sources in initial fingerprinting map generation, in: 2024 14th International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2024, pp. 1–6. https://doi.org/10.1109/IPIN62893.2024.10786156

[173] R. Hughes, L. Tao, I. Vallivaara, F. Alsehly, Calibration-free radiomap construction based on graph map matching, in: 2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2023, pp. 1–7. https://doi.org/10.1109/IPIN57070.2023.10332546

[174] Y. Hu, F. Qian, Z. Yin, Z. Li, Z. Ji, Y. Han, Q. Xu, W. Jiang, Experience: practical indoor localization for malls, in: Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, MobiCom '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 82–93. https://doi.org/10.1145/3495243.3517021

[175] D. Jaisinghani, R.K. Balan, V. Naik, A. Misra, Y. Lee, Experiences & challenges with server-side WiFi indoor localization using existing infrastructure, in: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 226–235. https://doi.org/10.1145/3286978.3286989

[176] Z. Gu, R. Bapna, J. Chan, A. Gupta, Measuring the impact of crowdsourcing features on mobile app user engagement and retention: a randomized field experiment, Manag. Sci. 68 (2) (2022) 1297–1329. https://doi.org/10.1287/mnsc.2020.3943

[177] D. Xu, C. Ruan, J. Cho, E. Korpeoglu, S. Kumar, K. Achan, Knowledge-aware complementary product representation learning, in: Proceedings of the 13th International Conference on Web Search and Data Mining, WSDM '20, Association for Computing Machinery, New York, NY, USA, 2020, p. 681–689.https://doi.org/10.1145/3336191.3371854

[178] Meta Analytics Team, Notifications: why less is more - how facebook has been increasing both user satisfaction and app usage, 2022, (https://medium.com/@AnalyticsAtMeta/notifications-why-less-is-more-how-facebook-has-been-increasing-both-user-satisfaction-and-app-9463f7325e7d). Accessed: 2025-04-07.

[179] Google Transit Partners, Transit crowd data: contributing data to improve transit info on google maps, 2023, (https://support.google.com/transitpartners/answer/9551309). Accessed: 2025-04-07.

[180] X. Zhang, X. Zhang, The mode of incentive control system, Enterprise Manag. Control Syst. China (2014) 275–296. https://doi.org/10.1007/978-3-642-54715-7_15

[181] Z. Zeng, J. Tang, T. Wang, Motivation mechanism of gamification in crowdsourcing projects, Int. J. Crowd Sci. 1 (1) (2017) 71–82.

[182] Z. Fitz-Walter, D. Tjondronegoro, Exploring the opportunities and challenges of using mobile sensing for gamification, in: N. Lane, F. Zhao, T. Choudhury (Eds.), Proceedings of the UbiComp 11 Workshop on Mobile Sensing: Challenges, Opportunities and Future Directions 2011, ACM Press, United States, 2011, pp. 1–5. https://eprints.qut.edu.au/48632/.

[183] G. Hsieh, Understanding and designing for cultural differences on crowdsourcing marketplaces, in: Proceedings of Chi, Crowdsourcing and Human-Computation Workshop, 2011, pp. 0–3. https://www.humancomputation.com/crowdcamp/chi2011/papers/hsieh.pdf.

[184] C. Riedl, J. Füller, K. Hutter, G.J. Tellis, Cash or Non-Cash? Exploring ideators' incentive preferences in crowdsourcing contests, J. Manag. Inf. Syst. 41 (2) (2024) 487–514. https://doi.org/10.1080/07421222.2024.2340828. https://doi.org/10.1080/07421222.2024.2340828 https://doi.org/10.1080/07421222.2024.2340828

[185] M. Ridge, S. Blickhan, M. Ferriter, A. Mast, B. Brumfield, B. Wilkins, D. Cybulska, D. Burgher, J. Casey, K. Luther, et al., 6. Understanding and connecting to participant motivations, The Collective Wisdom Handbook: Perspectives on Crowdsourcing in Cultural Heritage-Community Review Version (2021). https://britishlibrary.pubpub.org/pub/understanding-and-connecting-to-participant-motivations/release/1.

[186] T.Y.T. Suen, S.K.S. Cheung, F.L. Wang, J.Y.K. Hui, Effects of intrinsic and extrinsic motivational factors on employee participation in internal crowdsourcing initiatives in China, Sustainability 14 (14) (2022). https://doi.org/10.3390/su14148878

[187] A. Berke, R. Mahari, A. Pentland, K. Larson, D. Calacci, Insights from an experiment crowdsourcing data from thousands of US Amazon users: the importance of transparency, money, and data use, Proc. ACM Hum.-Comput. Interact. 8 (CSCW2) (2024). https://doi.org/10.1145/3687005

[188] B. Morschheuser, J. Hamari, J. Koivisto, Gamification in crowdsourcing: a review, in: 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 4375–4384. https://doi.org/10.1109/HICSS.2016.543

[189] A. Barredo Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. Garcia, S. Gil-Lopez, D. Molina, R. Benjamins, R. Chatila, F. Herrera, Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI, Inf. Fusion 58 (2020) 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[190] G. Cardone, A. Corradi, L. Foschini, R. Ianniello, ParticipAct: a large-scale crowdsensing platform, IEEE Trans. Emerg. Top. Comput. 4 (1) (2016) 21–32. https://doi.org/10.1109/TETC.2015.2433835

[191] A. Ray, C. Chowdhury, S. Bhattacharya, S. Roy, A survey of mobile crowdsensing and crowdsourcing strategies for smart mobile device users, CCF Trans. Pervasive Comput. Interact. 5 (1) (2023) 98–123. https://doi.org/10.1007/s42486-022-00110-9

[192] W.B. Qaim, A. Ometov, A. Molinaro, I. Lener, C. Campolo, E.S. Lohan, J. Nurmi, Towards energy efficiency in the internet of wearable things: a systematic review, IEEE Access 8 (2020) 175412–175435. https://doi.org/10.1109/ACCESS.2020.3025270

[193] J. Phuttharak, S.W. Loke, A review of mobile crowdsourcing architectures and challenges: toward crowd-empowered internet-of-things, IEEE Access 7 (2019) 304–324. https://doi.org/10.1109/ACCESS.2018.2885353

[194] R. Talla-Chumpitaz, M. Castillo-Cara, L. Orozco-Barbosa, R. García-Castro, A novel deep learning approach using blurring image techniques for Bluetooth-based indoor localisation, Inf. Fusion 91 (2023) 173–186. https://doi.org/10.1016/j.inffus.2022.10.011

[195] Á. Carro-Lagoa, V. Barral, M. González-López, C.J. Escudero, L. Castedo, Multicamera edge-computing system for persons indoor location and tracking, Internet Things 24 (2023) 100940. https://doi.org/10.1016/j.iot.2023. 100940

[196] W. Li, Z. Chen, X. Gao, W. Liu, J. Wang, Multimodel framework for indoor localization under mobile edge computing environment, IEEE Internet Things J. 6 (3) (2019) 4844–4853. https://doi.org/10.1109/JIOT.2018.2872133

[197] Z. Ding, W. Cao, Z. Zhang, Z. Wang, Y. Zhang, S. Yang, Edge computing empowered indoor positioning: a brief introduction, in: 2021 13th International Conference on Wireless Communications and Signal Processing (WCSP), 2021, pp. 1–4. https://doi.org/10.1109/WCSP52459.2021.9613444

[198] S. Li, Z. Qin, H. Song, C. Si, B. Sun, X. Yang, R. Zhang, A lightweight and aggregated system for indoor/outdoor detection using smart devices, Future Gener. Comput. Syst. 107 (2020) 988–997. https://doi.org/10.1016/j.future.2017.05. 028