Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.445 – 451

RESEARCH ARTICLE

MORE SMART, SECURED AND PRIVACY CONCERNED PARTICIPATION IN PARTICIPATORY SENSING

Ms. Sayara Bano Sheikh[1], Mrs. Preeti Deshmukh[2]

[1]Computer Technology, PCE, Nagpur, India
[2]Computer Technology, PCE, Nagpur, India
[1] sheikh.sayarabano@gmail.com; [2] preeti.deshmukh8@gmail.com

***Abstract*— Participatory Sensing (PS) is an arising archetype that focuses on the collection of data produced from a large number of connected, always-on, always-carried mobile devices. Sensing paradigm leverages humans as part of the sensing infrastructure. PS enables the distributed collection of data by self-selected participants to share local knowledge acquired by their mobile sensor equipped devices. Hence personal information of user is conveyed by reports. Thus, a number of privacy concerns may hamper the large-scale deployment of PS applications. In PS, the targets is to provide a high level of privacy and security to data producers like users who are providing sensed information and consumers like applications that are accessing the gathered information. In this article, we focus on privacy protection in PS and introduce an acceptable privacy-enhanced infrastructure. First, we accommodate a set of privacy requirements aiming at protecting privacy for both data producers and consumers. We present here a realistic architectural instantiation that attains privacy guarantees with provable security at very low additional computational cost and almost no extra communication overhead.**

***Keywords*— Participatory Sensing (PS), Privacy, Participant, Querier, Service Provider (SP), Registration Authority (RA)**

I. INTRODUCTION

The idea of a wireless sensor network (WSN) is not novel. WSN have many inexpensive wireless nodes, each one is capable of assembling, saving, and processing environmental information. The sensor nodes in a mesh co-operate and communicate with each other to carry out sensing task. WSN consists of spatially scattered self-directed sensors to observe physical or environmental conditions, like temperature, sound, pressure, etc. and to supportively pass the sensed information through the network to a principle area. Sensors are integrated in low-power devices which gather the information and conjointly perform processing in addition to connectivity with the genuine world. WSN is combined with the innovative ad hoc networking technology in order to facilitate inter-sensor communication. From the previous decade, researchers have envision the impact of WSN and expected the in depth installation of sensors, for ex, in buildings, rivers, forest or probably the atmosphere. The flexibility of establishing and configuring a sensor network is thus substantially advanced. This has triggered many of interest in many distinct WSN topics

As sensors abate pricey and extra widely offered, it's potential to plant in mobile devices enhances. [5]Mobile phone sensing is a growing. Sensor equipped mobile phones are staying close to the revolution in social networks, global green monitoring, personal and community healthcare, sensor augmented gaming, virtual reality and smart transportation systems. Fundamentally, Mobile phones have created a new stage for the data collection, discovery, and social analysis. Mobile phones are usually on and carried devices than any other previous personal technology. Mobile devices are progressively more equipped with the ability to sense the physical world (for example, through cameras, microphones, and accelerometers) and therefore network world (with Wi-Fi and Bluetooth interfaces) putting forward several opportunities for cooperative sensing applications.

Participatory sensing (PS) is a forthcoming model that targets the seamless collection of data from a large number of user-carried mobile devices which are embedded with sensors. PS collects the sensed data and provides the facts and figures about ecological tendencies such as urban traffic patterns, parking availabilities, pricing information, health related information, etc. PS is a new practice which makes use of the sensor equipped tools to collect and analyse data for use in social science, environmental and health discovery. Simultaneously, they deeply challenge our current understandings of privacy policy and data security.

II. PARTICIPATORY SENSING (PS)

A. What is PS?

Participatory sensing (PS) [1] is also known as urban sensing or opportunistic sensing or opportunistic people-centric. PS is revolutionary rising paradigm that focuses on the seamless collection of information from an outsized range of connected, always-on, always-carried devices. PS combines the availability and the state of being everywhere of mobile phones with sensing capabilities. PS refers to a mechanism by which the people collect, share and analyse native data. In PS [2], users with mobile devices (e.g., cell phones, laptops) participate in the collection of environmental information around them and submit the collected data to a central server for process, analysis, and storage. PS allows people to participate as a volunteer and sense their environment by means of close at hand sensor devices such as smart phones, and share this information with the existing cellular and Internet communication infrastructure.

PS [3] emphasizes the involvement of human being within the method of sensing. Several features of mobile devices make them a special and unprecedented tool for engaging participants in sensing their local environment. PS can draw on a range of mobile devices; the very first is their pure ubiquity across the demographic and geographic spectrum. The broad proliferation of mobile devices usage makes it doable to gather information. Through the global wireless network, people who wish to take part in PS scattered across a city or the world will simply coordinate and transfer information to servers wherever it is processed and integrated with different information. A small computational device carried by individuals in their day to day life sense information about human activity and directly or indirectly uploaded to server [3].

B. Why PS?

PS is used to make available the data which is not straightforwardly reachable to people. Generally user can get the needed information all the way through the internet. If the data is interrelated with the close at hand surrounding or about or near the housing area, then people can get the data effortlessly from other people. The data which is not discoverable through internet or by asking other people, in this picture PS sounds powerful. For example, Buddhist family can take the advantage of PS who wants to settle in an area of Tamilnadu where buddist majority is high. They, as a querier, can fire a query. A residential human of Tamilnadu can make available them this information.

III. PS PRIVACY NECESSITY

The abundance and the heterogeneity of entities in PS is an issue which is presently an increasing challenge [2]. In contrast to WSNs, sensing devices are no longer dull gadgets, owned by the network operator; in PS sensors are nothing but the personal devices that follow users at all time and their reports usually figures their personal information. Thus, not alone traditional security but additionally privacy issues need to look up, as there is always a fear of personal information disclosure. PS will pave because of novel distributed computing and new business models. However, PS is powerfully related to the number of users who are willing to devote device resources to sensing applications. Thus, wishing on giant and omnipresent user participation, PS will become effective provided that it'll protect the privacy of participating entities [3].

Issues like confidentiality or integrity ought to be strictly addressed [1]. As an example, all parties must be shielded from external eavesdroppers. The communications between two mobile devices and between mobile devices and servers should be completely confidential. Then again, the need for privacy protection is high because there is also a probability of the personal information leakage to internal adversaries. Indeed, because the Service Provider collects all information (i.e., reports and queries), it would learn an extensive amount of sensitive data regarding each mobile device, and therefore their privacy is at risk.

The continuous collection of information over long periods permits the Service Provider to meticulously profile users. Further, as data collected through PS applications becomes accessible to external entities and organizations (i.e., the Queriers), query interests also become sensitive and need to be hidden.

If users feel that their privacy is at risk, they can refuse to share their information. Particularly, it is required that the Service Provider performs report/query matching but learns no information concerning query interests. Also, data reports should not disclose any sensitive information to the Network Operator, the Service Provider or unauthorized mobile device participant about the entities which are involved in PS, any information about their identity and its location.

IV. PRIVACY ENHANCED PARTICIPATORY SENSING INFRASTRUCTURE (PEPSI)

PEPSI [1] [2] is a designed as a solution to provide privacy in PS application with respect to Mobile Node and Querier. Fig.1 depicts Participatory Sensing infrastructure which also described following terms:

A. PEPSI Architecture

1. Participant: The role of Participant is to provide the sensed data. The data collected from sensors is also called as report. Data is collected using sensor equipped mobile devices which are carried by voluntary participants
2. Querier: Queriers are the end users who are interested in receiving the sensed report using mobile devices.
3. Network operator (NO): The NO is liable for the communication infrastructure. NO provides network to collect and deliver sensor measurements (for ex, GSM or 3G).
4. Registration Authority (RA): RA manages Participant and Querier registration. RA routes reports specific matching to query to the Queriers.
5. Service provider (SP): The SP keeps a record of personal details of authorized Participant and Querier. SP also has a record of all reports submitted and query requested.

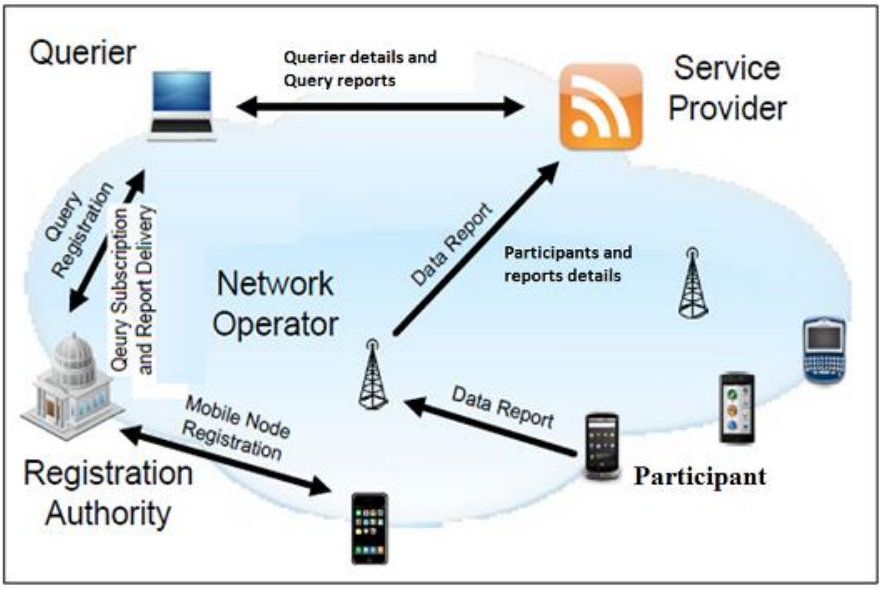

Fig. 1 Privacy-Enhanced Participatory Sensing Infrastructure

The main aim of PEPSI is to grant security to both Participant and Querier. PS must pay attention concerning the privacy of the participants that is Participant who provides sensed data and Queriers, uses that data, their privacy must not be in danger. In order to provide a high level of privacy, PEPSI introduces an entity called as Registration Authority (RA). RA sets up the system parameters and manages Participant and Querier registration. Participant and Querier register themselves to become authorized participants of PS. Hence only authorized participants can be a part of PS. Service Provider (SP) operates as a server which maintains a database of the entire authorized Participant and Querier and the data uploaded in PS.

V. PS APPLICATIONS

PS depicts the state of affairs of 'by the public and for the public'. Consider a paradigm [1], 'www.gasbuddy.com' is a PS application where gas prices are monitored from the reports and information speak out by participants and hence exposes their locations and movements. Few examples of PS application are explained below.

Iordanis Koutsopoulos [4] classifies the PS applications into three families: environment-centered, infrastructure and facility related, and socially or community centered. OpenSense[5] PS infrastructure is beneath 1st category performs real-time air quality monitoring and encompasses heterogeneous sensors. Example of the 2nd category is GreenGPS[6] that uses a vehicle interface to quantify and hand on fuel consumption and location data which is used to constructs fuel-efficient routes to destinations for querying users. Other example of 2nd class is CrowdPark[7] which facilitates parking slots from user submitted information and allows this information to assist alternative users find parking spots. In a system of the third category, LiveCompare[8] participants use their phone cameras to take a picture of the price tag of a product of interest. The other interested user receives pricing information for the product at nearby respective stores. One more example is DietSense[9], in which individuals take pictures of what they eat and share it within a community to compare eating habits, e.g. in a community of diabetics.

VI. PROPOSED WORK

PEPSI introduces the concept of RA and SP in order to provide privacy and security to Participant and Querier against unintended human being. PS is able to provide security in opposition to RA and SP and hence PS can be described as a smart PS.

A. *Using Advanced Encryption Standard (AES)* algorithm*:*

Advanced Encryption Standard (AES) algorithm is the building block of PEPSI. The AES is an encryption algorithm for securing sensitive material. AES encryption is used by U.S. for securing sensitive but unclassified material, so it is accepted that the algorithm is enough secure. AES is a symmetric encryption algorithm.

In PS state of affairs, Participant and Querier must have a warranty with the intention that their private ins and outs should not be untouched or pour out to any person. Hence selecting a precise cryptography tool could be a part of brooding. In PS, bulky participants are involved so adds overhead while selecting any cryptographic algorithm. By keeping all the above higher than issues in mind, AES algorithm is seen as the best suited algorithm for providing security and privacy in PS.

B. *Authorization of MN and Querier:*

If any user desires to participate in PS application, the prerequisite is to authorizing themselves first. RA deal with this authorization course of action. All the Participant and Queriers, initial of all, register them with RA. By providing a legitimate username and password, participant will be able to access PS. This is like any other email service, for example Gmail, where user can access their personal account, receive and forward mails, etc. Only authorized Participant can upload the reports and authorized Querier can get the requested query. SP also has a complete record of registered users.

Fig. 2 SP has Authorized Participant Record

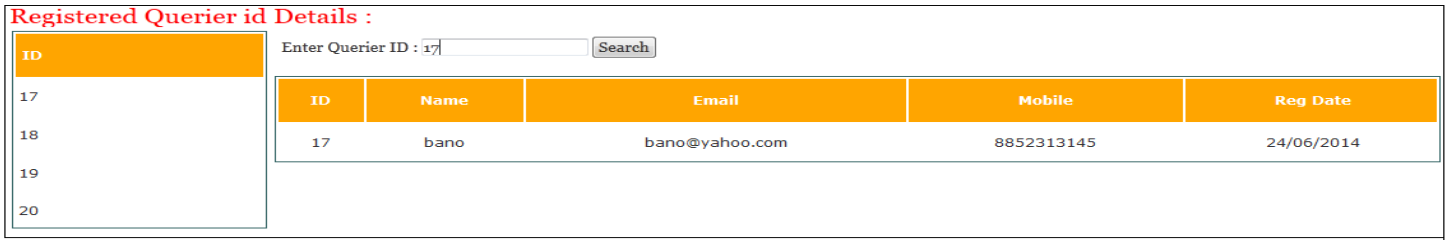

Fig. 3 SP has Authorized Querier Record

C. *Privacy of Participant and Querier:*

The responsibility of PS is to endow privacy and security to participants with regard to RA and SP as well. RA and SP both keep a replica of registered user personal details, reports and query profile, etc. The users must have the assurance that their personal details should not be misused by RA and SP and also not known to other people. Hence this is necessary to make participants believe that they are safe. This can be achieved by using AES algorithm. Using AES algorithm it is possible to hide

the identity and personal details of Participant and Querier. Participant and Querier are secured in opposition to RA, SP and other user by following means:

1) RA receives reports and query with the authorized user ID not with a user name. Also, RA loses the details as soon as it generates the matching key.

2) The personal details of Participant and Querier are stored in an encrypted form and the reports and query are stored in readable format to SP. As shown in the following fig the personal biodata of Participant and in fig personal biodata of Querier is secreted. Thus, it is not possible for SP to discover who submitted which data. SP also has a right to block those participants who always gives wrong information or uses abusive language. Once blocked, the Participant authorization is cancelled.

All Reports :

Name	Email	Mobile	Title	Value	Area	Description	Date	Block
[ï¯?¤¬ôù-±³U¹¿é	¾ ??rWS?¦XÛþ*±	ÎÿãPÐHæP×à°Ìp Ò?	population	10 k	nagpur	too much populated	28/06/2014 02:12:13	Block
·óÄ(¼Ø?4TZ	Ô?^±sa?XÚá æVÀÛ IpbúÄÍÈÊÛ	·?e@[??®6)?'	xerox center	10 paisa per page	kanhan	KOMAL xerox center offers services at a lowest price in kanhan,nagpur	29/06/2014 05:57:01	Blocked

Fig. 4 Participants and Uploaded Reports Details to SP

All Queries :

Name	Email	Mobile	Title	Area	Date
&K³£1±Éa?øÞ6	sYD2!«AñÀ?i]©oÆâ	ÉWå0ÆY` Ut?kÕA¶	population	nagpur	28/06/2014 02:14:18
&K³£1±Éa?øÞ6	sYD2!«AñÀ?i]©oÆâ	ÉWå0ÆY` Ut?kÕA¶	xerox center	kanhan	28/06/2014 02:14:44
ò½(#Znèò!ç»#¤3	+?¢³Ø?E+y}"³Ðq?Ô)hxú2Î²?U÷??3ù	ù@ñµ?K<ÈCV¤WìPh	train cancelled	nagpur to pune	29/06/2014 06:54:05
2dì3³0F?¼#«uu?§k	ÍÉ§¼??BZ«OK±£ âòJ§Ák~ïÀúÌ]-	LÀjEá¤=Øù?±??	food quality	hingna	29/06/2014 06:46:44

Fig. 5 Querier and Uploaded Queries Details to SP

3) Querier is incapable to uncover the Participant who uploaded the requested data. In the following fig, Querier receives the requested query but the name of the Participant who uploads the data is kept in an unreadable coded format. Hence the identity of participant is hidden.

Result : 1

Title : rainy sale **Area** : nagpur Posted By : µ½½F??`ú-

Answer :sale of womens garments Description :a good news for girls.purchase cloths at a 50% discount."rainy sale,near PNB,crp gate,hingna" Posted Date :01/07/20 03:54:10

Fig. 6 Participant Name is Unreadable to Querier

D. *Report/Query Matching:* Querier is able to search out their query if the same report is presented by Participant. Because there are bulky amount of reports in the database, it is obligatory to facilitate the Querier only demanded query, not additional information. Thus Report/Query Matching is mandatory to avoid overhead of Querier. RA carries out this Report/Query Matching. RA generate matching key meant for all report in the company of query. Querier is given matching key. Matching key performs the matching of requested query by the means of the reports. Once matched, the Querier will receive all the uploaded data satisfying his query. After receiving matching key, Querier is able to gain the requested and needed information.

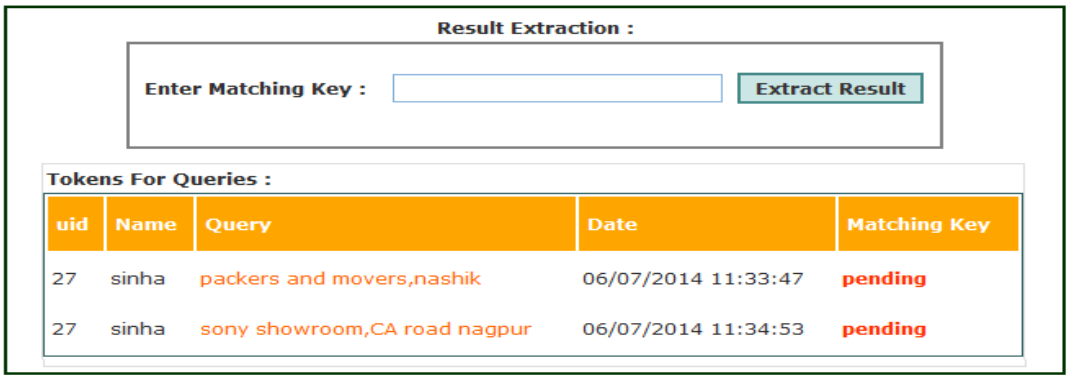

Fig.7 Querier Request Before Receiving Matching Key

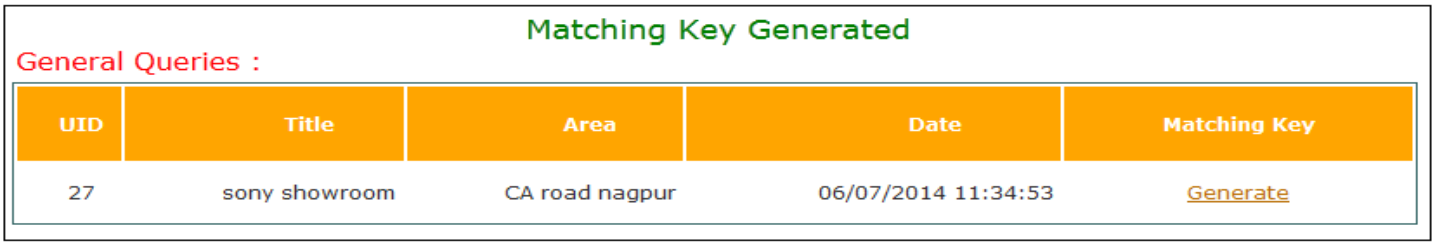

Fig. 7 RA Generates Matching Key for All Reports and Queries

The matching key test out whether the requested queries are on hand or say, whether uploaded by any participant. If the query is does not exist in database, at that moment every participant will receive a message to upload that report.

Fig. 8 Participant Receives a Message to Upload a Non Registered Query

Once the non registered query supplied by Participant, RA provoke matching key. Subsequent to reports matched with query, Querier can get the information by means of matching key.

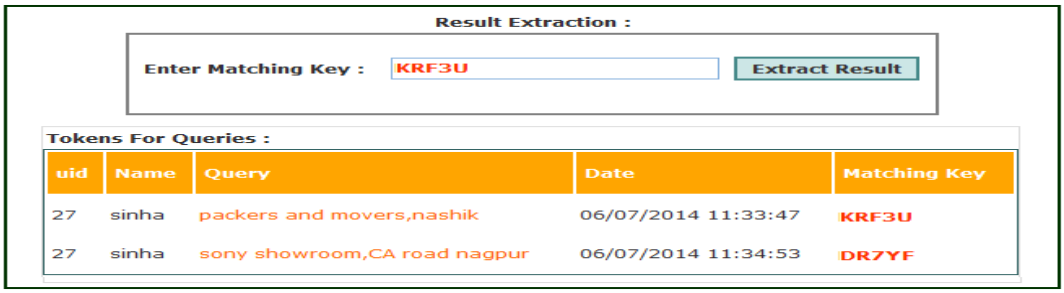

Fig.9 Querier Request After Receiving Matching Key

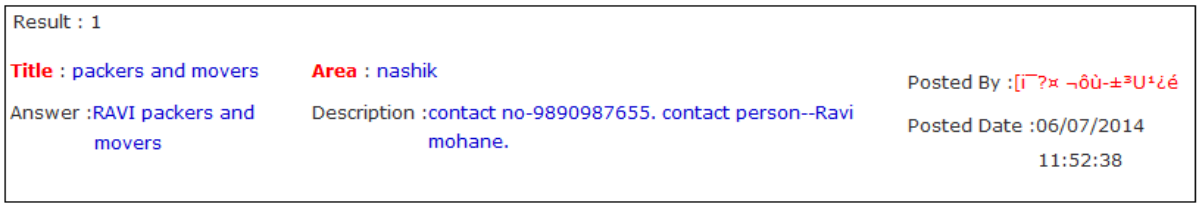

Fig.10 Querier Get the Requested Query Once Uploaded by Participant

VII. CONCLUSION

PS is a novel computing paradigm that bears an outstanding potential. If users are encouraged to contribute personal mobile device wealth, numerous applications and business models will crop-up. We projected the architecture of a privacy-preserving Participatory Sensing infrastructure and introduced an efficient cryptographic solution that achieves privacy with obvious security. In this paper PS, existing privacy situation in PS, security issues in PS and how more security can provide to PS is discussed. We claim without protecting the privacy of both data consumers and data producers, user participation can't be afforded. The solution presented in this paper can be adopted by current Participatory Sensing applications to enforce privacy and enhance user membership, with little overhead.

REFERENCES

[1] Claudio Soriente and Emiliano De Cristofaro, *Participatory Privacy: Enabling Privacy in Participatory Sensing*, IEEE transactions on networking NO.1 VOL.27 YEAR 2013
[2] E. De Cristofaro and C. Soriente, *Privacy-Preserving Participatory Sensing Infrastructure*, http://www.emilianodc.com/PEPSI/.
[3] Kapadia, A.; Kotz, D.; Triandopoulos, N., *"Opportunistic sensing: Security challenges for the new paradigm,"* Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International, vol., no., pp.1,10, 5-10 Jan. 2009 doi: 10.1109/COMSNETS.2009.4808850
[4]Koutsopoulos, I., *"Optimal incentive-driven design of participatory sensing systems,"* INFOCOM, 2013 Proceedings IEEE, vol., no., pp.1402,1410, 14-19 April 2013 doi: 10.1109/INFCOM.2013.6566934
[5] *OpenSense Project*: http://www.nano-tera.ch/projects/401.php, 2010
[6] R.K. Ganti, N. Pham, H. Ahmadi, S. Nangia, and T.F. Abdelzaher, *"GreenGPS: A Participatory sensing fuel-efficient maps application"*, in Proc. ACM MobiSys, 2010.
[7] T. Yan, B. Hoh, D. Ganesan, K. Tracton, T.Iwuchukwu, J.-S. Lee, *"CrowdPark: A Crowdsourcing-based Parking Reservation System for Mobile Phones"*, University of Massachusetts at Amherst Tech. Report, http://lass.cs.umass.edu/ yan/pubs/yan11CrowdPark.pdf
[8] L. Deng and L.P.Cox, *"LiveCompare: Grocery Bargain Hunting through Participatory Sensing"*, in Proc. ACM HotMobile, 2009.
[9] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin and M. Hansen, *"Image browsing, processing, and clustering for participatory sensing: Lessons from a dietsense prototype"*, in Proc. 4th Workshop on Embedded Network Sensors (EmNets), 2007.
[10] Chih-Jye Wang; Wei-Shinn Ku, *"Anonymous Sensory Data Collection Approach for Mobile Participatory Sensing,"* Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on pp.220,227, April 2012

