Security Mechanisms in Human Centered Smart Systems-Overview

S. Domi Evangeline[a] and Dr.G. Usha[b]

[a] Department of Computer Science and Engineering SRM Institute of Science and Technology Kattankulathur, Tamilnadu, India.

[b]Department of Software Engineering SRM Institute of Science and Technology Kattankulathur, Tamilnadu, India. ushag@srmist.edu.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Mobile crowd sensing is the process of sensing, carried out on behalf of the task provider by the user capable of completing the task. The user with their smart gadgets involves in the sensing process. This sensing process includes various applications geo-publicly supporting, monitoring, smart systems, etc. Since large number of users involved in crowd sensing process there is a threat for security both for the users and the data. In concern with the users both the task provider and the participant, issue a task or carry out the task issued based on the trust between each other. To pick up the task and carry out the task the participant must share their private details which may cause privacy issue to the participant. Whereas with the data the participants report at the completion of the task may be a false data or incomplete data. This cause a situation where the truthiness of the data is affected. This makes the complete process useless. These security issues like privacy, truth and trust must be addressed. In order to provide a clear idea of Crowd sensing network a taxonomical approach is followed to classify the network based on the data involved and various participants. Based on the various participants, the malicious users in the crowd sensing network is classified and the security issues caused by them are addressed.

Keywords: Security, Crowdsensing, Privacy, Trust, Truth.

1. Introduction

Crowd sensing is a methodology including an enormous, spread out gathering of members utilizing smart gadgets with the point of getting solid information from the field. Gadgets furnished with different sensors have gotten pervasive. Most mobile phones can detect encompassing light, noise (through the receiver), location (through the GPS), movements (through the accelerometer), and the sky is the limit from there. These sensors can gather huge amounts of information that are helpful in many ways. For instance, GPS and accelerometer information can be utilized to find potholes in urban areas, and amplifiers can be utilized with GPS to map pollution in a location. Mobile crowd sensing has a place with three primary functionalities: ecological, (for example, observing contamination), infrastructure, (for example, finding potholes), and social, (for example, following activity information inside a community). Mobile crowdsensing happens in three phases: data assortment, data storage and data upload. Data assortment draws on sensors accessible through the Internet of things. There are three primary procedures for gathering this data: physically, physically with control, based on predefined settings. Data detecting is activated by a specific setting that has been predefined (e.g., a gadget starts to gather information when the user is at that location at a specific time). The main contribution is organized as follows: 1. Taxonomical classification of crowdsensing network based on the data that is involved in the crowd sensing network and the types of participants involved in the system. 2. Analyze various types of malicious users present in the system that cause the security issues in the crowd sensing network. 3. Various solutions given so far for security issues like privacy, trust and truth between various participants in crowd sensing network is studied. The paper is organized as follows. II section explains the overview of the crowd sensing environment. With the process of CS, Classification of CS network. III section discuss about system architecture of CS network. Section IV discusses challenges faced by the CS network. V section discusses about the various types of malicious users in CS network. VI section discusses security analysis of CS network and the last section concludes the paper.

2. Overview Of Crowd Sensing

Process of Crowd Sensing

Crowd sensing (CS) is the process where many people from the crowd involve in the completion of the tasks. The task provider publishes his task in the network as an open call. The user based on the gadget available to him to complete the task picks up his/her task and complete it on behalf of the task provider. The task provider when he publishes a task, he specifies his rules to complete the task in an agreement. The user reads the agreement and picks up the task and carries out the process. There are multiple users involved in the task and sends back the result they recorded to task provider. Task provider accumulates all the results and defines his result of the task. The task provider based on the performance of the user return him with the payment he quoted in the smart contract. The quick rise of smart gadgets, for example, cell phones and wearables with many numbers of sensors, empowers another method for getting sensor information, known as crowd sensing. Together with the natural mobility of their users, the capacity to obtain neighborhood information from individuals' environmental condition or even about themselves is gained.

Classification of CS Network

The CS network is classified based on the data and participants. Based on the data it is divided into three types (i) spatial CS (ii) temporal CS (iii) spatio-temporal CS. Based on the participants it is divided into two types. They are, (i) Participatory CS (ii) Opportunistic CS is explained in the Fig. [1].

Spatial crowd sensing (SC) depends on the spatial data of the users who senses the data's in the process of sensing. SC is specific about the location.

Temporal CS is crowd sensing experiments on temporal information. The property of crowd sensor is mobility which act as a major feature of the user with respect to their functional and non-functional aspects of various applications that can be done by the user.

However, there are many challenges faced by the crowd sensing network because of their dynamic, volatile and highly distributed nature while including the features of both spatio-temporal data. When the CS process focus on these data as their key parameters in the query to the sensor cloud it is called as saptio-temporal CS. Next, we will discuss about the types of the crowd sensing network on the basis of the types of participants involved in sensing.

Participatory CS involves voluntary participation of the user. The user based on his/her interest and available resources to complete the task, chooses the task. They involve in the task with full commitment and involvement.

Opportunistic CS is the process in which the user is involved in the task unknowingly or unintentionally. But the user is participating in the task without his/her knowledge. In next section we will discuss about various challenges faced by the crowd sensing network.

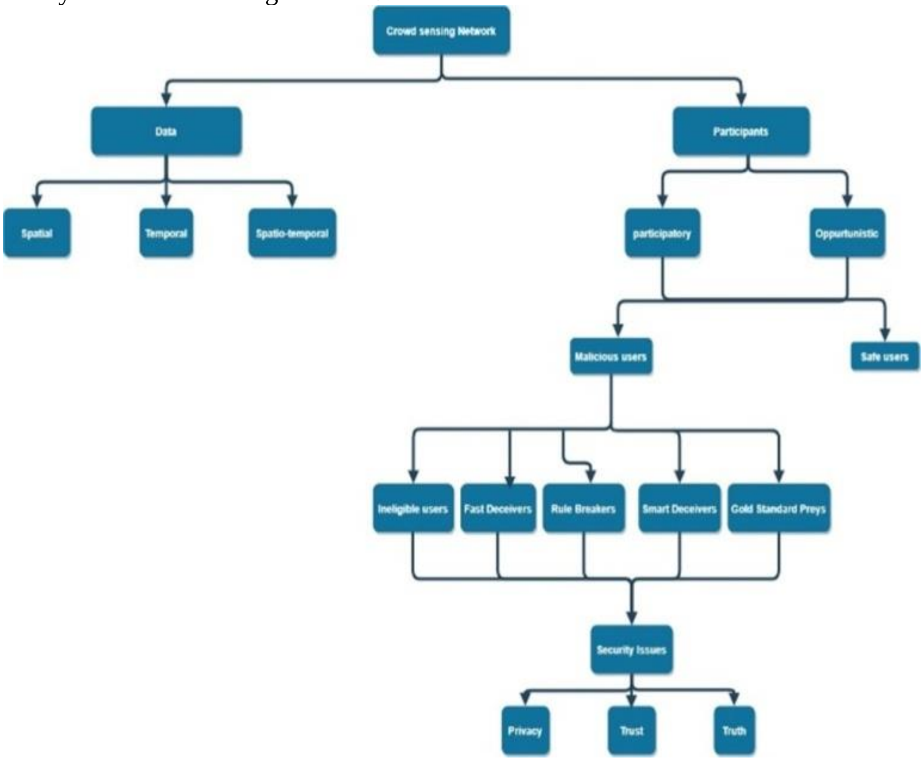

Figure 1. Taxonomical classification of crowd sensing network

3. System Architecture Of Cs Network

System Model

There are three main platform on which the process is carried out. They are (i) aggregator platform (ii) crowd provider platform (iii) specialized platform. There are two main participants involved in the CS process. They are (i) task provider (ii) user.

Interactions in CS Platform

The participants with the special gadgets form the lower level of the crowd sensing process. The users with these special sensors sense the data and carry out the process of data collection based on each task they choose to do. The participants who carry out the same function in the network cloak together into a specialized platform. The other tasks which requires participants to carry out the process waits in the crowd provider platform. The task provider uploads his tasks with the other resources and smart contract into the crowd provider platform.

The large task is divided into many small numbers of microtasks. These microtasks are chosen by the participants based on the type of information he provides in return agreeing the smart contract. The aggregator platform does the process of storing all microtasks of a task into a single task. And on the submission of the reports by the participants accumulates the reports of each micro task by various users into a single microtask report. The reports of various microtask of the same task are also combined by the aggregator in aggregator platform.

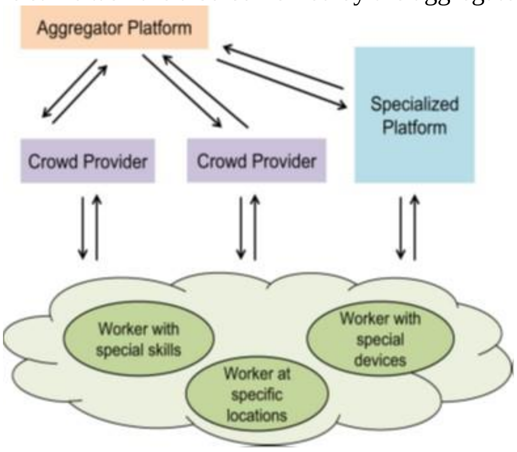
Aggregator Platform
Specialized Platform
Crowd Provider
Crowd Provider
Worker with special skills
Worker with special devices
Worker at specific locations

Figure 2. Interactions in crowdsensing platform

4. Challenges Faced By Cs Network

One of the major challenges faced is Resource limitations. The resources like energy, bandwidth, and computation capacity of the various input devices that user uses for the task completion are to be managed efficiently.

Leveraging the differences between the sensory devices to enhance the quality of the data and report using minimum resource is a novel challenge.

Data integrity can also be a problem people can either unintentionally or maliciously contribute false data. If the participant is opportunistic participant, he/she without any intention in order to complete his process he may fill in false data. Or else if the participant is a malicious user, he intentionally fills the network with false data.

Security infers protecting accumulated data and MCS systems from unauthenticated access, use, revelation, interference, adjustment and damage.

Privacy ordinarily implies the capacity of a substance to decide if, when, and to whom the data about the element is to be discharged or uncovered.

Trust is the certainty, conviction, and assumption about the unwavering quality, trustworthiness, capacity, and different attributes of the CS network.

Since there are multiple users involved in the process of sensing same task the data reported by them vary from one another. The truthiness of the data is questionable.

Next, we will study about various types of malicious users present in the crowd sensing network that causes various security issues.

5. Malicious Users In Cs Network

Based on the analysis of the implicit behavioral patterns of malicious users and their data reports presence of five different types of malicious users are present in the CS network.

The aspects that are being analyzed are (i) the criteria of eligibility for a user to access the resources to do the task, (ii) whether responses from the task doer satisfy the predefined rules, or (iii) whether response report meets the quality level expected by the task provider.

Based on these aspects the malicious users are categorized into following five types (i) Ineligible users (ii) fast deceivers (iii) Rule breakers (iv) smart deceivers (v)Gold Standard Preys.

Ineligible Users (IE) are the malicious users who do not follow the pre-requisites that are stated by the task provider when the task is being created along with the task description. Fast Deceivers (FD) are the malicious users with the goal of acquire cash effectively and rapidly by misusing the access.Rule Breakers (RB) are the malicious users who do not wait for the task provider’s validation message in response for each response. Smart Deceivers (SD) are the malicious users who try deceiving the administrators by acting like they stick on the rules. Gold Standard Preys (GSP) are the users who are malicious adhere to the directions along with substantial reaction to be given but neglect to pass the standard necessity of the task provider. They show non-malicious behavior, but fail to pass the best quality level test. . Next, we will categorize the various types of security issues caused by these malicious users in the crowd sensing network.

6. Security Analysis Of Cs Network

Three main security issues involved in the CS network are (i) trust (ii) privacy (iii) truth.

Privacy is a rule implies the capacity of a substance to decide regardless of whether, when, and to decide regardless of whether, when, and to whom the data about the element is to be discharged or uncovered. The privacy of the user cannot be guaranteed by the server as the sever itself may attempt to provide a recovery method to the user which can be used by the unauthenticated user to extract the user details without his consent.

Trust alludes to a circumstance wherein two people certainly trust each other even though they have not recently settled an individual relationship.. At the point when trust is available, key trades among people with individual connections give an incredible instrument to guarantee secure correspondences.

Truth is very much important feature of the network. This is a feature that explains about the truthiness of the data entered by the various users. The users involve in completing the tasks by reporting the results they inferred in carrying out the process. The data entered by the users reflect on the overall result of the task. The correctness of the report submitted by the user has to be verified.

These security issues and various mechanisms to provide security against these issues are tabulated in table 6.1, 6.2& 6.3.

Table 6.1. Overview of Privacy Preserving Mechanisms

Reference number	**Proposed work**	**Achievement**	**Limitation**
[8]	An implicit and continuous Authentication method is proposed	An exact and effective nonstop validation technique for security delicate mobile applications utilizing contact-based conduct biometrics	Validation without the prerequisite of user attention and specific equipment is carried out.
[9]	Security issues are addressed using a blockchain based safeguard mechanism	The system ensures area data as well as ensures reasonable exchanging without the requirement for a confided in outsider	Reusing of the datas downloaded by the user who can act as a malicious user is an issue
[10]	Social connection of the user is used in game framework with three party	The privacy of the data is protected using game with three parties between users, task provider and adversary	Security spillage is an extreme danger to users
[11]	A protection mindful assignment distribution and information collection plot is proposed Utilizing bilinear matching and homomorphic encryption	Oblivious transfer protocol proposed to achieve privacy	Fog nodes are always considered to be authorized
[12]	Security safeguarding task suggestion	Encryption of online/readiness data to enhance the quality of encryption	It is based on the assumption that the system is authorized system

Table 6.2. Overview of Trust Providing Mechanisms

Reference number	**Proposed work**	**Achievement**	**Limitation**
[1]	Analysis of security in CS network	Three main ways to improve trust. Color based scheme, rank based scheme, report based	Did not develop for the timeline-based system
[5]	Secure and accountable Participatory Sensing with SPPEAR architecture	The privacy of the user even against multiple malicious PS servers and multiple malicious users.	Publicly supporting feature is not considered.
[6]	A reliable publicly supporting model in SIoT	A mechanism providing reputation familiar with a mechanism to analyse the dependency property of each user publicly.	User population is increasing tremendously has to be well managed.

[7]	A novel methodology	An epic, proficient, and viable methodology, is acquainted with identify noxious user.	The user based on the location is not considered.
[13]	An epic, proficient, and viable methodology, is acquainted with identify noxious user in ale scale informal organizations.	The framework needs to plan an impetus system that energizes all user in the system to take an interest in the location of the pernicious client.	The users have diverse action

Table 6.3. Overview of Truth Evaluation Mechanisms

Reference number	Proposed work	Achievement	Limitation
[2]	Analyzing various cheaters in CS.	Interface dependent evaluation-based on the innovative way the user work with the task.	Anonymous nature of the cheaters is not considered
[3]	The reports are validated by the participants.	The validation of the submitted report is carried out with the two mechanisms as follows. The majority decision approach, the control group approach to rate the users.	The data of the user is not considered
[4]	analyzed the truth of information in CS network	protection against privacy of the participants.	provide feedback ensures the security of the information

7. Conclusion

In this study, we have analysed the various types of malicious users in the crowdsensing network that cause various types of malicious attacks that affect the privacy trust and truth of the network. We have analysed the various existing methodologies and algorithms that have be aroused in this 10 year of time with respect to the privacy, trust and truth. Many works have been concentrating in the privacy issues only. The truth and trust issues has been concentrated less comparing these three issues. As a conclusion of this analysis, the security protection in crowd sensing network is still in its infancy; thus, there are multiple open issues that can be worked and solved soon.

References

1. A.C. Weaver, J.P. Boyle, L.I. Besaleva, "Applications and trust issues when crowdsourcing a crisis", 21st international conference on computer communications and networks (ICCCN), pp. 1-5, 2012.
2. C. Eickhoff, A.P. de Vries, "Increasing cheat robustness of crowdsourcing tasks", Information retrieval, Vol. 16, No. 2, pp. 121-137, 2013.
3. M. Hirth, T. Hoßfeld, P. Tran-Gia, "Analyzing costs and accuracy of validation mechanisms for crowdsourcing platforms", Mathematical and Computer Modelling, Vol. 57, No. 11-12, pp. 2918-2932, 2013.
4. L. Cilliers, S. Flowerday, "Information security in a public safety, participatory crowdsourcing smart city project", World Congress on Internet Security (WorldCIS-2014), pp. 36-41, 2014.
5. S. Gisdakis, T. Giannetsos, P. Papadimitratos, "SPPEAR: security & privacy-preserving architecture for participatory-sensing applications", Proceedings of the ACM conference on Security and privacy in wireless & mobile networks, pp. 39-50, 2014.
6. K. Wang, X. Qi, L. Shu, D.J. Deng, J.J. Rodrigues, "Toward trustworthy crowdsourcing in the social internet of things", IEEE Wireless Communications, Vol. 23, No. 5, pp. 30-36, 2016.
7. G. Yang, S. He, Z. Shi, "Leveraging crowdsourcing for efficient malicious users detection in large-scale social networks", IEEE Internet of Things Journal, Vol. 4, No. 2, pp. 330-339, 2016.
8. Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, X. Zhou, "BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics", Ad Hoc Networks, Vol. 84, pp. 9-18, 2019.

9. M. Yang, T. Zhu, K. Liang, W. Zhou, R.H. Deng, "A blockchain-based location privacy-preserving crowdsensing system", Future Generation Computer Systems, Vol. 94, pp. 408-418, 2019.
10. K. Li, L. Tian, W. Li, G. Luo, Z. Cai, "Incorporating social interaction into three-party game towards privacy protection in IoT", Computer Networks, Vol. 150, pp. 90-101, 2019.
11. H. Wu, L. Wang, G. Xue, "Privacy-aware task allocation and data aggregation in fog-assisted spatial crowdsourcing", IEEE Transactions on Network Science and Engineering, Vol. 7, No. 1, pp. 589-602, 2019.
12. W. Tang, K. Zhang, J. Ren, Y. Zhang, X.S. Shen, "Privacy-preserving task recommendation with win-win incentives for mobile crowdsourcing", Information Sciences, Vol. 527, pp. 477-492, 2020.
13. Dr.G. Usha, S. Kannimuthu, Vinoth Nas, H. Karthikeyan, "Augmentation and Orchestration of Security Techniques in Fog Computing", International Journal of Recent Technology and Engineering, Vol. 8, No. 2S4, pp. 143-148, 2019.
14. G. Usha, S. Kannimuthu, P.D. Mahendiran, A.K. Shanker, D. Venugopal, "Static analysis method for detecting cross site scripting vulnerabilities", International Journal of Information and Computer Security, Vol. 13, No. 1, pp. 32-47, 2020.