International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Location Based Privacy Using Cloaking Algorithm

Rohit Kamalay[1], Kundan Kumar[2], Lalit Sagar Rachala[3], Montu[4],

Mrs. Sowmya S R[5]

rohitkamalay04@gmail.com [1] , kundankrsingh2014@gmail.com[2] , sagar.rachala20@gmail.com[3] , guliamontu19@gmail.com[4], srs.is.08@gmail.com

Department of Information Science and engineering, Dayananda Sagar Academy of Technology And Management, Bangalore, India
Faculty in Department of Information Science and Engineering, Dayananda Sagar Academy of Technology And Management, Bangalore, India

***Abstract*— Participatory sensing is a type of data collection that relies on the participation of individuals to gather data about a particular environment or phenomenon. One important aspect of participatory sensing is preserving the privacy of the individuals who are participating in the data collection process. This can be particularly challenging in applications where location data is being collected, as this type of data can be highly sensitive and revealing. Inthis literature survey, we will explore the various approaches that have been proposed to address location privacy in participatory sensing applications.**

***Keywords*— K anonymity, Location Based Services (LBSs), Location Privacy, Voronoi diagram (VD).**

INTRODUCTION

One common approach to preserving location privacy in participatory sensing is the use of privacy-preserving data collection techniques. These techniques aim to minimize the amount of sensitive location data that is collected, and to protect the privacy of individuals by masking or obfuscating their location data. Examples of privacy-preserving data collection techniques include the use of location perturbation, which addsnoise to the location data to make it less precise; the use of location cloaking, which hides the location of individual users behind a "cloak" of aggregated data; and the use of location aggregation, whichcombines the location data of multiple users to obscure the movements of individual users.

Another approach to preserving location privacy in participatory sensing is the use of privacy-enhancing technologies (PETs). PETs are designed to protect the privacy of individuals by enabling them to control the collection, use, and disclosure of their personal data. Examples of PETs that have been proposed for use in participatory sensing include privacy-enhancing protocols, which allow individuals to selectively share their location data with specific parties; privacy-enhancing platforms, which provide a secure and confidential environment for the accumulation and analysis of location information; & privacy-enhancing applications,which enable individuals to customize their privacysettings and control the flow of their location data. In addition to these technical approaches, there arealso a number of legal and policy frameworks that have been developed to address location privacy in participatory sensing. These frameworks ofteninvolve the establishment of clear rules and regulations governing the collection, use, anddisclosure of location data, as well as the development of mechanisms for enforcing these rules and holding organizations accountable for anyprivacy violations.

II. Literature Survey

Preserving location privacy in participatory sensing is a complex and challenging problem, as it requires balancing the need to collect accurate and useful data with the need to protect the privacy of individuals. While there are a number of approachesthat have been proposed to address this issue, it is important for organizations and individuals to carefully consider the privacy implications of any participatory sensing application, and to adopt appropriate measures to ensure that the privacy of participants is respected.

Different methodologies can be used to implement the cloaking algorithm to cloak the exact location of a user.

1. Anonymizer

K-anonymity can be defined as a technique which ensures identity protection of a person in a dataset by making sure that there are at least K other individuals with similar characteristics in the dataset. In the context of location privacy, K-anonymity should protect the identity of individuals by ensuring that their location data is not unique or easily identifiable.

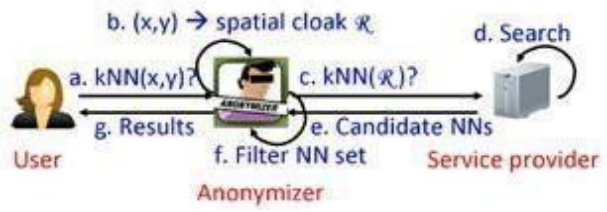

Fig.1. A view of K anonymous location privacy. Here NN represents the nearest neighbour. kNN represents kth nearest neighbor query.

One way to accomplish K-anonymity for location data is by using location perturbation, which adds noise to the location data to make it less precise while another approach to achieving K-anonymity for is by implementing location aggregation, which combines the location data of multiple individuals to obscure the movements of individual users.

2. Trusted Third Party And Function Generator

A trusted third party (TTP) could potentially be used to facilitate the exchange of location data in a way that preserves privacy. For example, the TTP could act as a mediator between a location-based service and a user, receiving requests for location data from the service and then obtaining the necessary data from the user in a secure andprivacy-preserving manner. The TTP could alsoensure that the location data is used only for thepurposes for which it was intended and is notshared or disclosed to any other parties without theuser's consent.

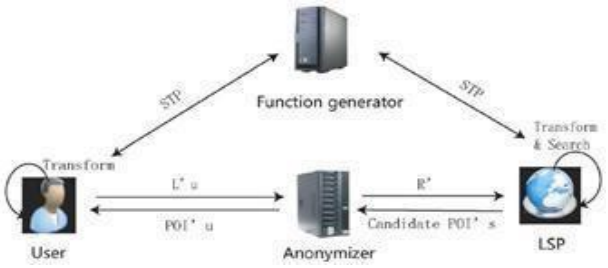

Fig.2. Enhanced location privacy preserving system (ELPP) used for privacy of the user. R' represents transformed ASR.

A function generator could potentially be used in the development of a system that uses location data in a privacy-preserving manner. For example, the generator could be used to test the performance of algorithms that are designed obscuring or encrypting location data such that it makes it difficult for unauthorized parties to identify the user's precise location. The generator could also be used to testthe reliability and accuracy of such algorithms under several conditions.

It is necessary to know when using a trusted third party (TTP) or a function generator alone might not be enough to ensure the privacy of user's location data. There are a number of other technical, legal, and policy considerations that must also be taken into account when designing a system that handles location data in a privacy-preserving manner. For example, it may be necessary to implement additional security protocols to protect the data from unwarranted access or tampering, and to make sure that this data will be used for purposes for

which it was intended. It may also be necessary to comply with relevant privacy laws and regulations, and to obtain the user's consent before collecting or using their location data.

3. Privacy Preserving Identification Mechanism

Privacy preserving identification mechanisms could be used to protect the privacy of location data in several ways. Suppose a pseudonymizationscheme could be used for replacing user's actuallocation with a pseudonym which represents thelocation, while still allowing the user to beidentified and tracked. This could enable location-based services to offer personalized recommendations or other features withoutrevealing the user's exact location data to the network provider or any other third parties.

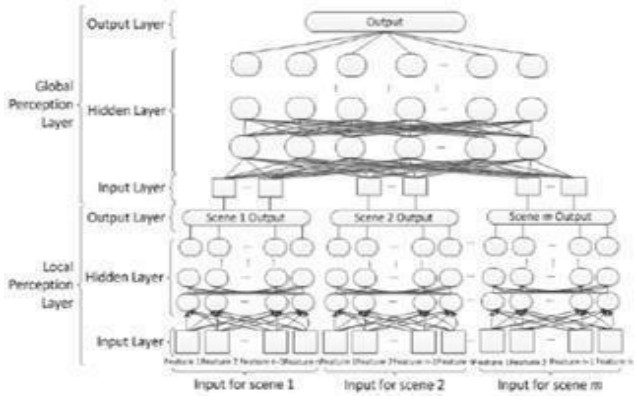

Fig.3. Diagrammatic representation 2-Layer ANN model.

Tokenization could also be used to protect the privacy of location data by replacing the actual location with a randomly generated token that has no inherent meaning. This could make it more difficult for unauthorized parties to determine the user's location, while still allowing the user to be identified and tracked by the service provider.

Zero-knowledge proofs could be used in a similar manner, allowing the user to prove their location to a verifier without actually revealing their location. This could enable location-based services to offer personalized recommendations or other features without disclosing the user's location to the network provider or any other third parties.

It is worth noting that no single identification mechanism is foolproof, hence its always possible that location data could be revealed through some means. However, by carefully designing and implementing a privacy preserving identification mechanism, it is possible to greatly reduce the risk of location data being disclosed unnecessarily.

4. Spatiotemporal Blurring

Spatiotemporal blurring is a method which is used to preserve the privacy of location data by obscuring or "blurring" the precise location of an individual or device. The goal of spatiotemporal blurring is to enable location-based services to provide useful and personalized recommendations or other features without having to reveal the exact location of the user to any other third parties.

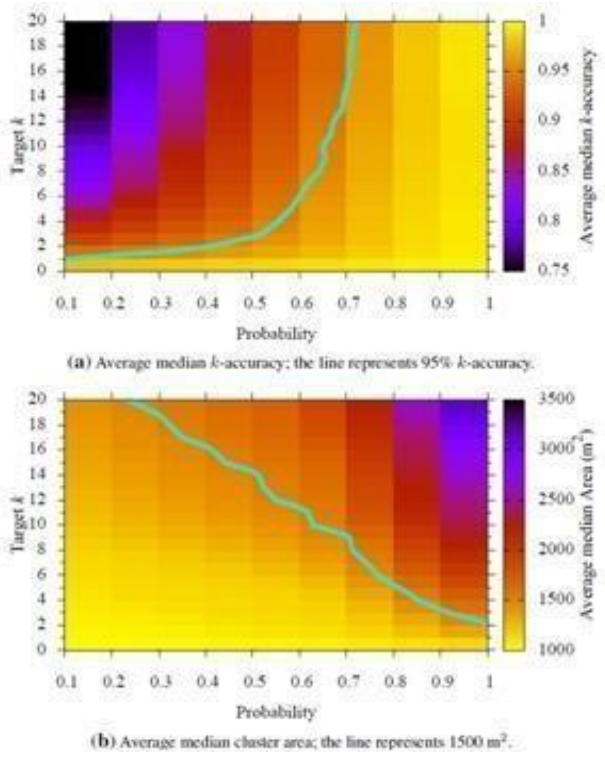

Fig.4.Target k vs. probability p.

There are a number of different approaches to implementing spatiotemporal blurring, and the specific method to implement depends on specific needs and requirements of the application. Some common approaches include:

Geofencing: This involves defining a geographic area, or "fence," around a location and then blurring or obscuring the location of any individuals or devices that fall within the fence. The size and shape of the fence can be customized to balance the level of privacy protection with the need for accurate location information.

Randomization: This involves randomly "jittering" the location of an individual or device within a certain area, making it more difficult for unauthorized parties to determine the exactlocation. The size of the area can be adjusted to balance the level of privacy protection with the need for accurate location data.

K-anonymity: This involves grouping individuals or devices into "anonymity sets" based on theirlocation, and then only disclosing the location of the anonymity set as a whole rather than the location of any individual member. The size of the anonymity sets can be adjusted to balance the level of privacy protection with the need for accuratelocation data.

Spatiotemporal blurring can be implemented in a number of different ways, including through the use of software algorithms, hardware devices, or a combination of both. For example, a smartphoneapp could use geofencing or randomization to blur the location of the user, while a wearable device could use k-anonymity to group the user with other individuals in the same location.

There are a number of benefits to using spatiotemporal blurring to protect the privacy of location data. One of the main benefits is that it allows individuals to use location-based services without needing to reveal their exact location to the service provider or any other third parties. This can help to prevent the service provider from building a detailed profile of the user's movements and habits, which could be used for targeted advertising or other purposes.

Another benefit of spatiotemporal blurring is that it can help to inhibit the unauthorized release of location data. For example, if a hacker were to gain access to a database of location data, the use of spatiotemporal blurring could make it more difficult for them to determine the exact location of any individual or device. This can help to reduce the risk of identity theft, stalking, or other types ofprivacy violations.

However, it's worth noting that spatiotemporal blurring is not a perfect solution, and there are a number of limitations and challenges that must be taken into account when using it to protect the privacy of location data. One of the main limitations is that it can reduce the accuracy of the location data, which may make it less useful for certain applications. For example, if the size of the anonymity set or the "jitter" area is too large, it may be difficult for a location-based service to provide accurate recommendations or other features.

Another challenge is that spatiotemporal blurring may not be effective against more advanced attacks, such as those that use machine learning or other techniques to infer the location of an individual or device from partially obscured data. In these cases, it may be necessary to use additional privacy preserving techniques in order to provide a higher level of protection.

5. Anonymous Data Reporting Protocol

Anonymous data reporting protocols are privacy-enhancing technologies (PETs) that allow individuals to share their location data with others in a way that preserves their privacy. Theseprotocols typically involve the use of cryptographic techniques, such as anonymous credentials orzero-knowledge proofs, to enable individuals to share their location data without revealing their identity.

One example of an anonymous data reporting protocol for location privacy is the Location Privacy Protocol (LPP), which was developed by researchers at the Massachusetts Institute of Technology (MIT). The LPP allows individuals to share their location data with third parties in a way that preserves their privacy, while also enabling third parties to authenticate the integrity of thelocation data. This is achieved through the use of

anonymous credentials, which enable individuals to prove that they are in a particular location without revealing their identity.

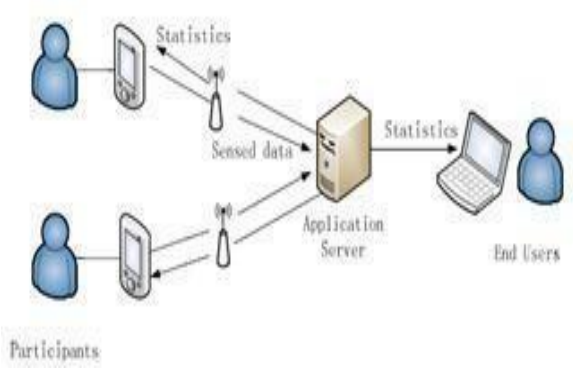

Fig.5. System architecture

III. Conclusion

One of the main advantages of location cloaking is that it can be effective at preserving the privacy of individuals in location data, even when the data is being collected and analyzed by third parties. This is because the cloaking techniques can make it difficult or impossible for third parties to identify the location data of individual users, even if they have access to the aggregated data.

However, there are also some limitations to location cloaking. One of the main limitations is that it could reduce the preciseness and usefulness of the location data, because cloaking techniques can make it less precise or less detailed. This can make it difficult to use the data for certain types of analysis or applications.

Overall, location cloaking can be a helpful technique for preserving the privacy of individuals in location information, particularly in participatory sensing applications where the data is being collected from many different sources. Although, it is necessary to carefully consider the trade-offs between privacy and accuracy when using location cloaking, and to select the right cloaking method based on the specific needs of the application.

References

[1] Chow, Chi-Yin & Mokbel, Mohamed & Liu, Xuan. (2006). A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Service. 171-178. 10.1145/1183471.1183500.

[2] Latanyasweeney,. (2012). ACHIEVING k-ANONYMITY PRIVACY PROTECTION USING GENERALIZATION AND SUPPRESSION. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 10. 10.1142/S021848850200165X.

[3] Gruteser, M. & Grunwald, Dirk. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. Proceedings of the 1st International Conference on Mobile Systems, Applications and Services. ACM. 31-42.

[4] Sweeney, L.. (2002). k-Anonymity: A Model for Protecting Privacy. IEEE Security and Privacy. 10. 1-14.

[5] Ackerman, Linda & Kempf, James & Miki, Toshio. (2003). Wireless location privacy: A report on law and policy in the United States, the European Union, and Japan. All Rights Reserved.

[6] Meyerson, Adam & Williams, Richard. (2004). On the Complexity of Optimal K-Anonymity.. Proceedings of the ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems. 23. 223-228. 10.1145/1055558.1055591.

[7] B. Gedik and Ling Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), 2005, pp. 620-629, doi: 10.1109/ICDCS.2005.48.

[8] T. Peng, Q. Liu and G. Wang, "Enhanced Location Privacy Preserving Scheme in Location-Based Services," in IEEE Systems Journal, vol. 11, no. 1, pp. 219-230, March 2017, doi: 10.1109/JSYST.2014.2354235.

[9] Khuong Vu, Rong Zheng and Jie Gao, "Efficient algorithms for K-anonymous location privacy in participatory sensing," 2012 Proceedings IEEE

INFOCOM, 2012, pp. 2399-2407, doi: 10.1109/INFCOM.2012.6195629.

[10] J. Liu, X. Li, R. Sun, X. Du and P. Ratazzi, "An Efficient Privacy-Preserving Incentive Scheme without TTP in Participatory Sensing Network," 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422848.

[11] Dimitrios Tsolovos. Enforcing Privacy in Participatory Sensing Systems. Middleware Doctoral Symposium 2018, ACM, Dec 2018, Rennes, France. ⟨hal-01910067⟩

[12] Mokbel, M. F., Chow, C. Y., & Aref, W. G. (2006, September). The new casper: Query processing for location services without compromising privacy. In *VLDB* (Vol. 6, pp. 763-774)

[13] Duckham, Matt & Kulik, Lars. (2005). A Formal Model of Obfuscation and Negotiation for Location Privacy. Lecture Notes in Computer Science. 3468. 152-170. 10.1007/11428572_10.