International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Location Based Privacy Using Geotagging 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[5]

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*— Location-based privacy is an important aspect of modern applications that utilize user geolocation data. This abstract presents a solution for location-based privacy using a cloaking algorithm. The algorithm aims to protect the privacy of users by obfuscating their precise location while still providing relevant location-based services. The proposed system leverages the Geolocation API and the Leaflet library to obtain and display the user's current position on a map. The algorithm dynamically adjusts the user's displayed location by introducing a small random displacement, ensuring that the user's exact location remains concealed. The system also incorporates measures to handle user consent and provide accurate estimations of location accuracy. By implementing this cloaking algorithm, location-based applications can strike a balance between personalized services and user privacy, enhancing the overall user experience and maintaining user trust.**

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

I.INTRODUCTION

The use of privacy-preserving data collecting techniques is one popular method for protecting location privacy in participatory sensing. These methods are designed to preserve people's privacy by masking or obscuring their location data and to reduce the quantity of sensitive location data that is gathered. Location cloaking, which conceals the location of specific users behind a "cloak" of aggregated data, location perturbation, which adds noise to the location data to make it less precise, and location aggregation, which combines the location data of various users to hide the movements of specific users, are a few examples of privacy-preserving data collection techniques.

Using privacy-enhancing technologies (PETs) in participative sensing is another strategy for protecting location privacy. By giving people choice over the gathering, using, and disclosing of their personal information, PETs are intended to preserve people's privacy. Examples of PETs that have been suggested for use in participatory sensing include privacy-enhancing protocols, which allow people to selectively share their location data with particular parties, privacy-enhancing platforms, which offer a secure and private environment for the accumulation and analysis of location information, and privacy-enhancing applications, which let people customize their privacy settings and control the flow of their location data. A number of legal and legislative frameworks have been established to handle location privacy in participatory sensing in addition to these technical techniques. These frameworks frequently entail the creation of precise guidelines and standards that regulate the gathering, use, and sharing of location data as well as the creation of systems for enforcing these guidelines and holding companies responsible for any privacy violations. Location-based services have become a crucial aspect of our everyday lives in the current digital world. These services provide useful features including location-based targeted marketing, personalized suggestions, and aid with navigating. However, privacy issues are raised by the gathering and use of accurate geolocation data. Due to possible concerns, such as unauthorized surveillance, profiling, or exploitation of personal information, users may be reluctant to divulge their precise position.

II. LITERATURE SURVE

Participatory sensing privacy protection is complicated and difficult issue to solve since it calls for juggling the demands of gathering accurate and relevant data with those of maintaining individual privacy. Although numerous solutions have been put forth to deal with this problem, it is crucial for businesses and individuals to carefully consider the privacy implications of any participatory sensing application and to take the necessary precautions to guarantee that participant's privacy is respected.

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

1. Anonymizer

K-anonymity is a strategy that protects a person's identity in a dataset by ensuring that there are at least K other people with comparable features in the collection. K-anonymity should safeguard individual identities in the context of location privacy by guaranteeing that their location data is neither distinctive or readily recognizable.

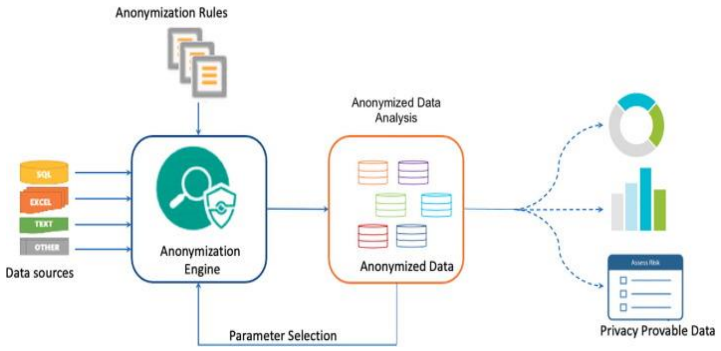


Fig.1. A view of K anonymous location privacy.

Location perturbation, which reduces the precision of the location data by adding noise to it, is one method for achieving K-anonymity for location data. Location aggregation, on the other hand, combines the location data of many users to hide the movements of specific users.

2. Third Party Reliable and Function Generator

The communication of location data may be facilitated in a fashion that protects privacy via a trusted third party (TTP). For instance, the TTP may serve as a go-between between a location-based service and a user, taking requests for location data from the service and securely and privately acquiring the required information from the user. The TTP might also make sure, that the location data is only shared or released with third parties with the user's permission and that it is used only for the reasons for which it was intended.

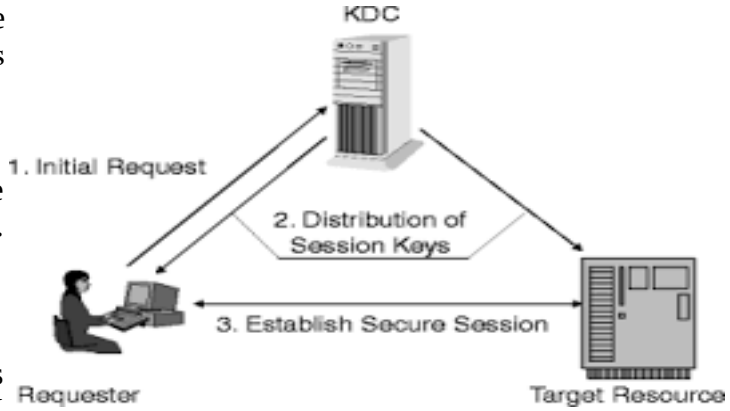


Fig.2. Enhanced location privacy preserving system (ELPP) used for privacy of the user. R' represents transformed ASR.

3. Geotagging Cloaking Algorithm (GCA)

It works by adding random noise to the latitude and longitude of a user's location data. This technique prevents precise location tracking while still providing useful information about a user's general location. It creates a set of cover areas around a user's location, rather than a single point. This technique makes it more difficult to determine a user's precise location. This project has been developed in context as a proof of concept and illustration for obfuscation techniques over GPS position. As the man in the middle attack, the web application works by interposing itself between websites and the browser. It acts transparently by adding noise to the GPS positions exchanged.

Websites can request an access to your location through browser defined methods. Our web application provides privacy within a defined area by adding noise to your real position, making it less precise. The privacy level defined in options determines the amount of noise added to your real location. A noised position is privacy preserving, however location-based services provided by websites would be less useful.

4. Spatial Cloaking Technique

Spatial cloaking is a privacy mechanism that is used to satisfy specific privacy requirements by blurring users' exact locations into cloaked regions. This technique is usually integrated into applications in various environments to minimize the disclosure of private information when users request Location-based service. Since the database server does not receive the accurate location information, a set including the satisfying solution would be sent back to the user. General privacy requirements include K-anonymity, maximum area, and minimum area.

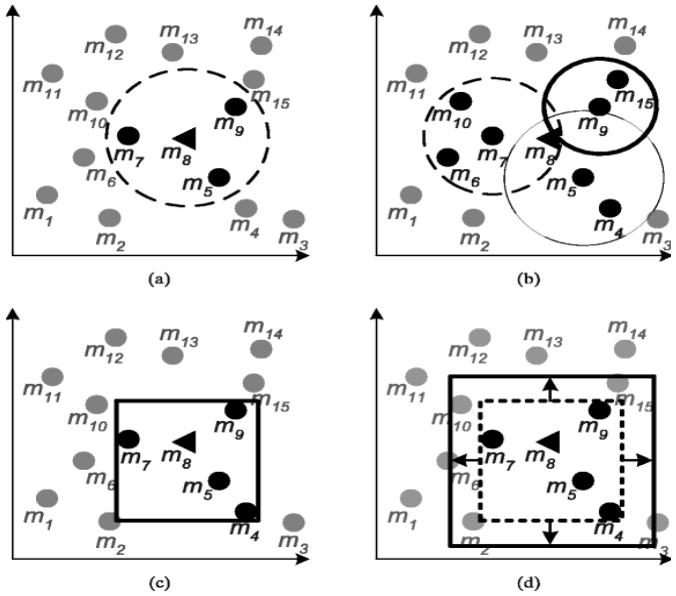


Fig.3. Spatial cloaking techniques

III.METHODOLOGY

The methodology for implementing location-based privacy using a cloaking algorithm involves several key steps.

System Design and Requirements:

Define the objectives and requirements of the location-based privacy system. Identify the target platform(s) and technologies to be used. Determine the desired level of location obfuscation and user control over privacy settings.

Data Collection and Geolocation API:

Utilize the Geolocation API to retrieve the user's current location. Implement mechanisms to handle user consent for accessing and sharing location data. Set up error handling and fallback options in case geolocation data is unavailable.

Map Integration and Cloaking Algorithm Implementation:

Integrate a mapping library, such as Leaflet, to display the user's location on a map interface. Configure the map to visually represent the user's location accurately, while concealing the precise coordinates using the cloaking algorithm. Develop the cloaking algorithm that introduces controlled random displacements to obfuscate the user's true location. Define the algorithm's parameters, such as the range and distribution of displacements, to ensure a balance between privacy and usefulness of location-based services. Apply the algorithm to the user's location data before displaying it on the map interface.

User Interface and Controls:

Design and implement a user interface that allows users to manage their privacy settings. Provide options for users to adjust the level of location obfuscation or disable location sharing altogether. Incorporate mechanisms to obtain and handle user consent for specific location-based services.

Accuracy Estimation:

Implement mechanisms to estimate the accuracy of the displayed location based on available geolocation data. Communicate the accuracy information to the user, providing transparency and aiding decision-making regarding the use of location-based services.

Testing and Validation:

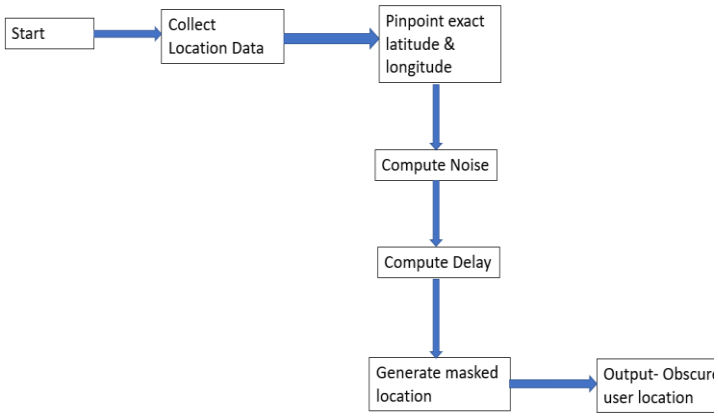
Conduct rigorous testing of the system, including various scenarios and edge cases, to ensure proper functionality and privacy protection. Validate the effectiveness of the cloaking algorithm in preserving user privacy while maintaining the usability of location-based services.

Deployment and User Feedback:

Deploy the location-based privacy system on the target platform(s) and make it available to users. Gather user feedback and conduct user surveys to assess the system's usability, privacy effectiveness, and

overall user satisfaction. Incorporate user feedback to make improvements and refinements to the system, if necessary.

Design Methodology



IV. CONCLUSION

This project is an attempt at improving user's location privacy. The ability to effectively protect individual privacy in location data, even when the data is being gathered and analyzed by other parties, is one of the key benefits of location cloaking. This is due to the fact that, even if they have access to aggregated data, cloaking techniques can make it difficult or impossible for third parties to identify the location data of specific users.

In the future, this project could be improved by incorporating some of the following innovations-

Differential Privacy: Future location-based services could use differential privacy techniques to protect users' location data while still allowing aggregate statistics and insights to be generated.

Homomorphic Encryption: cryptographic technique that allows data to be processed without being decrypted. Location data could be encrypted before it is sent to location-based services, and the services could still perform analysis and provide recommendations based on the encrypted data.

Federated Learning: machine learning technique that allows models to be trained on decentralized data. In the context of location-based services, this could mean that the models used to generate recommendations could be trained on data from individual users' devices rather than being trained on a centralized server. This would allow users to keep their location data on their own devices while still benefiting from the insights generated by the service.

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] Latanya Sweeney, (2012). ACHIEVING k-ANONYMITY PRIVACY PROTECTION USINGGENERALIZATION 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/INFOCOM.2012.6195629.