SN Computer Science (2020) 1:174
https://doi.org/10.1007/s42979-020-00178-z

SURVEY ARTICLE

A Survey on User's Location Detail Privacy-Preserving Models

M. B. Rajashekar[1] · S. Meenakshi Sundaram[1]

Received: 13 April 2020 / Accepted: 20 April 2020 / Published online: 16 May 2020
© Springer Nature Singapore Pte Ltd 2020

Abstract

Protecting personal information of users is a challenging task in the area of computer network security in the recent days. Personal information of users is highly essential to provide location-based services (LBS), and at the same, it is important to protect it from unauthorized users. Users cannot avoid the sharing of location information in the current era of social networks. In order to provide continuous LBS, personal data of the users are required. When users want to use social networks, they worry about preserving their privacy. Users normally prefer to maintain their location secure and safe in social networks for many privacy reasons. Security cracks in social network lead to tracking of user location, and they may misuse user's data. In this paper, we present different techniques that are used to protect location privacy of the users. Also it helps us to select an appropriate technique to protect location information of the user.

Keywords Location-based services · Computer network security · Location privacy · Social networks

Introduction

Today's digital world attracts more number of users to use Internet for various applications. Users are continuously engaged online for different activities and also to get different services from the outside world. Thus, protecting personal information of the users has become a challenging task. Since cost-effective smart phones have become popular, people have started using this technology for many kinds of services. The mobile networks are not secure due to their broadcasting nature. Secure services in mobile networks are less as mobile nodes join and leave the network at any point of time in a location.

Due to increase in smart phone users, the demand for location-based services (LBS) has also increased. The LBS provides information based on the location of the user, which is provided by the user mobile. Global position system (GPS) is a location detection device which stores coordinate information of users in a location-based server by enabling the users. Service providers provide location-based information even in the case of lack of accuracy. Location-based games, friend-finder applications and place reviews require large amount of location information of users to provide the service. If the collected location information is not secure, then unauthorized people can access user's private information and there is a possibility of tracking the user's activity. This information may help unauthorized users to keep track of detailed activities of users and predict their daily movements. Today, most of the social applications use location information of the users to provide different features. Users need to update their location information in order use social applications. Available location features of smart phones help the social applications to collect large quantities of location information of users; hence, privacy is the challenging task for smart phone users.

The collected location information helps the service providers to find exact location of the user at any point of time and to trace the movement of users. User-provided information during registration in social application helps the service providers to find users' interest in the future. This information is analyzed statistically, and it is stored for a longer duration. Knowledge of location information of the users helps the providers to learn more about them, and they are intended to sign up again. Spatial and temporal cloaking

This article is part of the topical collection "Advances in Computational Approaches for Artificial Intelligence, Image Processing, IoT and Cloud Applications" guest edited by Bhanu Prakash K N and M. Shivakumar.

✉ M. B. Rajashekar
rajashekar@gsss.edu.in

[1] Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Affiliated to VTU, Belagavi, Karnataka, India

techniques were used to access the location-based services as shown in Fig. 1 [1].

Today, different ways are found by the unauthorized users to misuse the location information for gaining profit by gathering legal evidence and by economic and physical stalking. Hence, secure and strong privacy policies are required for today's social network than the available polices. Providing the strong security for location information is a major concern, and it is the duty of providers to protect it from unauthorized users. Many researchers are working on this problem for the past few years, and they have suggested providing the privacy to location information using different techniques. In this paper, we present different methods that are suggested by the researchers to provide the privacy in location-based service.

Related Works

Zhang et al. developed a method for users and LSP to introduce several anonymizers between them and combine with the different mechanisms and technologies such as dynamic pseudonym, Shamir threshold and *K*-anonymity to improve the content privacy in continuous LBSs and users' trajectory. This architecture improved the user's privacy and performance [14, 18].

Huang et al. [15] proposed a scheme to realize the content privacy and location privacy to encode index elements by adopting scheme called prefix membership verification. Different encoding elements are *DBtree* construction algorithm, query processing algorithm and trapdoor generation. It was also proposed that the attackers can be diverted by using optimization scheme such as *DBtree* index element encoding and traversal optimization.

Shahid et al. [16] developed a method for location privacy with the help of I-diversity, privacy area preservation and *k*-number of locations. The proposed method improves the privacy against the inference attacks. It extensively minimizes the delay for successive queries in spatiotemporal domain.

Pu Has et al. proposed scheme uses the LBS provider and fog server to maintain user's privacy. To provide the integrity and confidentiality for request and response data, both AES and one-time pad key and IBE were used. It also opposes the attacks such as colluding attacks, external attacks and internal attacks.

Analysis and Discussions

In this section, based on the related works, analysis has been carried out for location-based services and privacy preserving.

Analysis of Privacy-Preserving Scheme

Gruteser et al. [1] presented usage of spatial and temporal cloaking for location-based services, in which spatial and temporal cloaking techniques were used to access the location-based services. These techniques help to maintain the location information from the unauthorized by sending estimated values of time and location to the server instead of correct values.

Srinivasan et al. [2] presented a fingerprint image enhancement using fuzzy-based filtering technique, in which cloaking was achieved with pseudonyms and silent times. This will change the device identifiers regularly, and data could not transmit in regular intervals for a long duration.

Mokbel et al. [3] proposed a privacy location-based database server, which provides the user's privacy by protecting the arbitrators and trusted services.

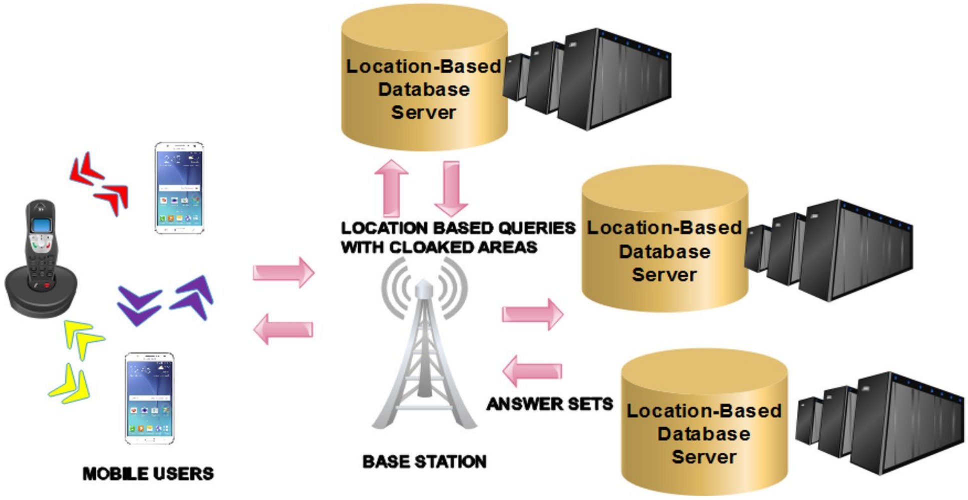
Location-Based Database Server
Location-Based Database Server
Location-Based Database Server
LOCATION BASED QUERIES WITH CLOAKED AREAS
ANSWER SETS
BASE STATION
MOBILE USERS

Fig. 1 Spatial and temporal cloaking system for location-based services

Papadopoulos et al. [4] presented strong location privacy for nearest neighbor search, in which strong location privacy is provided using private information retrieval (PIR). Any location in the data space a query indistinguishable can be done by using K nearest neighbor (KNN), and strong location privacy notation is defined. Query plan and PIR functionality are the main two components of this method. During the execution, the same number blocks must be retrieved by the query. If the database contains N sequential blocks which are maintained by the server, then PIR protocol gets back the ith block from the server by enabling the client [19].

Mascetti et al. [5] proposed a centralized privacy-preserving computation of users' proximity, in which location coordinates information is obtained and is transformed to be protected from servers. The longitude protocol provides the centralized solution based on the privacy-aware to the three-party secure communications between the server and each buddy. Every time service provider gets the user location, and it uses two-dimensional area for representation. The dimension depends on the requirement of the user's privacy with respect to buddies. Solutions obtained two-dimensionally are converted into equivalent zooidal space. Projection of buddy A in the toroidal space is done by applying solid transformation, and the result of this is sent to the service provider. Solid transformation is determined by sharing with each user the secret of their buddies. The proximity is computed by the service provider in the toroidal space, and then the result is communicated with the participating buddies to compute the two-dimensional space proximity [19].

Motani et al. [6] presented a wireless virtual social network, in which how people will use the social network to gather the information is discussed.

To improve the system performance, three metrics were identified.

1. Time taken to locate a match.
2. Number of matches found by a query.
3. Probability of a match.

Swap and spread are the two simple models, which describe the propagation of query within a bazaar. This architecture can be incorporated with the present cellular infrastructure easily.

Gedik and Liu [7] presented providing location privacy for mobile systems, in which location privacy is achieved against various privacy threats using personalized k-anonymity model. Many numbers of users get the support of location k-anonymity with the sensitive personalized privacy requirements to define privacy personalization framework. Each mobile node in the network has to follow the framework, and it makes to specify the minimum level of anonymity, maximum temporal and spatial resolutions, it helps to accept when requesting for k-anonymity preserving location-based services (LBSs). The location security broker on a trusted server runs the message perturbation engine and mobile users' location anonymization, like spatial–temporal cloaking of location information and identity removal. The efficient algorithms such as spatiotemporal cloaking called clique cloak were designed to offer personalized high-quality location k-anonymity, and before forwarding any request to LBS providers, location privacy threats must be reduced or avoided.

Narayanan et al. [8] presented location privacy via private proximity testing, in which proximity of privacy-preserving tests is discussed. Several protocols have been used to test privacy-preserving proximity at different levels of granularity. The required location tags have been generated in order to build up the security of proximity testing from the physical environment. Generated location tags were unpredictable, and they were derived from different electromagnetic signals existing in the environment, like Bluetooth and Wi-Fi. They helped to share the entropy among all users at a given time and in a given location. The developed system was implemented on the android platform, and effectiveness was reported. This system managed the public keys through the social networks.

Ghinita et al. [9] presented a PRIV´E: anonymous location-based queries in distributed mobile systems, in which user's anonymity was preserved using decentralized architecture by issuing spatial queries to LBSs.

Hoh et al. [10] presented how to enhance the privacy and security in traffic monitoring systems. Achieving the address privacy was a challenging task, and this was done by separating the authentication tasks and communication from sanitization and data analysis. Architecture assigned filtering functions, actual data analysis and authentication to separate entities to resolve the tension between privacy and data integrity. Data like vehicle's identity was known by entity but other information such as position and speed information was not accessible. On the other hand, entity knows the speed and position but it does not have information about identity. Encryption was done on the information to minimize the node compromise risk and data sanitization to increase the data integrity.

Beresford and Stajano [11] presented how to enhance user's privacy in location-based services, in which long-term user movement tracking was prevented. The model contained the trusted middleware system which was located between untrusted third-party and underlying location system. Middleware in the geographic space application register was called as application zone. Users had registered in geographic regions, and middleware limited the location information such as location sightings inside the application zone-registered users. There were some geographic regions where the user movements could not be traced by any applications in such regions which were called mix zones. If any user enters into mix zones, then their identity mixes with all user identities in a mix zone. Boundary line was defined between an application zone and mix zone as the border.

Baden et al. [12] discussed how to provide user-defined privacy in online social network, in which user may obtain the information from online social network called persona. Attribute-based encryption (ABE) is used by the persona to hide the user data. It also helps to create effective applications, in which private data are accessed through a defined policy. User of persona needs to generate a pair of key and the public key distributed among all users to share the data, and private key is kept secret. Based on the relationship defined by the user, other users are considered as friends. Creation of group among the several users is allowed by the persona. Personal data of user are encrypted, and they cannot be accessed by all users in a group. Persona also allows to exchange the data between users with certain restrictions. Users were able to join the group using arbitrary criteria, but we suggest choosing the group based on their relationship such as co-worker or neighbor.

Comparative Study of Privacy Preserving Using Location-Based Services

See Table 1.

Challenges Faced by Privacy Preserving Using Location-Based Services

See Table 2.

Open Research Challenges

1. Accuracy and correctness are not as expected. Security attacks on this mechanism can easily break the user's privacy.

Table 1 Comparative study for privacy preserving

Ref. No	Year of publication	Name of the authors	Techniques	Shortcomings
[1]	2015	"M. Gruteser and D. Grunwald"	"Spatial and temporal cloaking"	Accuracy and correctness are not as expected
[2]	2016	"K. Srinivasan and C. Chandrasekar"	"Gaussian filter and high boost filter"	Disconnects the users and Strict functionality
[3]	2016	"M. F. Mokbel, C.-Y. Chow, and W. G. Aref"	"privacy-aware query processor and location anonymizer: Casper"	Exposed of private data
[4]	2017	"S. Papadopoulos, S. Bakiras, and D. Papadias"	"Retrieval of Private Information"	Performance degradation
[5]	2017	"S. Mascetti, C. Bettini, and D. Freni"	"Longitude protocol"	Range queries are not appropriate for moving objects
[6]	2017	"M. Motani, V. Srinivasan, and P. S. Nuggehalli"	"Swap and spread models"	No detail study of security aspect of network
[7]	2017	"B. Gedik and L. Liu"	"Protecting location privacy using *k*-anonymity model"	Degrading results
[8]	2017	"A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh"	"Cryptographic protocols"	Problem while applying to geo-social applications
[9]	2018	"G. Ghinita, P. Kalnis, and S. Skiadopoulos"	"Decentralized architecture for preserving the anonymity of users"	Annotation imposed and ordering challenges not addressed
[10]	2018	"B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady"	"Techniques of Data suppression"	User's privacy may break by the different attacks on the server
[11]	2018	"A. Beresford and F. Stajano"	"Mix zones—subscribers messages and delays using an anonymity service"	Reveal approximate real-world location to the servers in plaintext
[12]	2018	"R. Baden, A. Bender, N. Spring, B. Bhattacharjee"	"Data Encryption on servers"	Unsatisfactory in location privacy protection
[13]	2018	"T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno"	"Preserving the ability to track stolen or lost devices by provides strong guarantees of location privacy"	Useful for recovering own information, but it will not help to recover the information of their associates

Table 2 Challenges faced by privacy-preserving methods

Research paper	Method used	Support public auditing	Support privacy preserving	Support data dynamics	Support batch auditing	Maintain integrity of data	Maintain confidentiality of data
"Privacy preserving public auditing for data storage security in cloud computing"	"HLA with random masking"	'Yes'	'Yes'	'No'	'No'	'Yes'	'No'
"Privacy preserving public auditing for secure cloud storage"	"HLA with BLS signature"	'Yes'	'Yes'	'No'	'Yes'	'Yes'	'No'
"Privacy preserving public auditing for secure cloud storage"	"HLA with BLS signature"	'Yes'	'Yes'	'No'	'Yes'	'Yes'	'No'
"Enabling public auditing and data dynamic for storage security in cloud computing"	"HLA with BLS signature along with MHT"	'Yes'	'Yes'	'Yes'	'Yes'	'Yes'	'No'
"Toward secure and dependable storage services in cloud computing"	"Homomorphism tokens +eraser code"	'Yes'	'Yes'	'Yes'	'No'	'Yes'	'No'
"Secure and efficient privacy preserving public auditing for cloud storage"	"HLA with BLS signature"	'Yes'	'Yes'	'No'	'Yes'	'Yes'	'No'
"Cloud server storage using TPA"	"Mercle has tree"	'Yes'	'Yes'	'Yes'	'No'	'Yes'	'No'
"privacy preserving public auditing service for data storage in cloud computing"	"MHT + RSA algorithm"	'Yes'	'Yes'	'No'	'No'	'Yes'	'Yes'
"Privacy preserving & batch auditing in secure cloud data storage using AES"	"HLA with random masking + AES Algorithm"	'Yes'	'Yes'	'No'	'Yes'	'Yes'	'Yes'
"Privacy preserving public auditing in cloud using HMAC algorithm"	"HMAC algorithm"	'Yes'	'Yes'	'No'	'No'	'Yes'	'No'

2. The malicious administrators or trusted servers can easily expose private data. Configuration errors or software bugs are still open issues in maintaining location privacy and preserving.
3. In longitude, in order to permit the users to make known the location information to their friends, the transformation is maintained secretly between the pair of friends. Users can disclose their location only to subset of their friends maintaining location privacy and preserving.
4. Since passwords are so widely used, they have become obsolete. Passwords are not only difficult to manage but also insecure because they can be easily guessed or cracked by hackers. Protecting passwords is an open issue.
5. Furthermore, if business uses passwords to protect internal accounts and user database, the user's sensitive data could be at risk.
6. Mobile users hierarchical clustering is used by the PRIV´E, but challenges of annotation imposed and total ordering requirements have not been discussed [17].
7. Protecting user's anonymity and location privacy is still an open challenge.
8. Another interesting open issue is with regard to user interfaces. On the one side, very simple tools should be provided to define LBQIDs and verify them based on statistical data. On the other side, simple and effective interfaces are needed to specify the level of anonymity required by the user, as well as to notify when identifi-

cation is at risk. Graphical solutions like the open and closed lock in an Internet browser should be considered.

Conclusion

In location-based services, it is required to develop a new model which addresses the new attack and threats to break the privacy of users. These new models need to overcome the disadvantages of existing ones. Novel solution approaches could combine different proposed solutions, to compensate for the disadvantages of certain models with the advantages of others. Increasing location-enabled devices and maintaining the user's privacy in location-based services are the challenging tasks. The location details of the user must be protected from unauthorized access to avoid misuse of information.

This paper compares the different techniques which are used to provide privacy in location-based services, and also issues and methodologies of various techniques were discussed. This paper also helps the researchers to understand issues associated with different techniques which maintain privacy in location-based services. A detailed survey has been done in this paper in respect of parameters such as integrity and confidentiality. Also various techniques related to CP-ABE methods to analyze issues related to security aspects have been discussed.

Funding This research work has not received any funding from any organization.

Compliance with Ethical Standards

Conflict of interest All the authors of this paper declare that there is no conflict of interest.

References

1. Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of Mobisys, 2015.
2. Srinivasan K, Chandrasekar C. An efficient fuzzy based filtering technique for finger-print image enhancement. In: AJSR, ISSN 1450-223X, No. 43, pp. 125–140, 2016.
3. Mokbel MF, Chow C-Y, Aref WG. The new casper: a privacy aware location-based database server. In: ICDE, 2016.
4. Papadopoulos S, Bakiras S, Papadias D. Nearest neighbor search with strong location privacy. In: PVLDB, 2017.
5. Mascetti S, Bettini C, Freni D. Longitude: centralized privacy preserving computation of users' proximity. In: Proceedings of SDM, 2017.
6. Motani M, Srinivasan V, Nuggehalli PS. Peoplenet: engineering a wireless virtual social network. In: Proceedings of MobiCom, 2017.
7. Gedik B, Liu L. Location privacy in mobile systems: a personalized anonymization model. In: Proceedings of ICDCS, 2017.
8. Narayanan A, Thiagarajan N, Lakhani M, Hamburg M, Boneh D. Location privacy via private proximity testing. In: Proceedings of NDSS, 2017.
9. Ghinita G, Kalnis P, Skiadopoulos S. Prive: anonymous location based queries in distributed mobile systems. In Proceedings of WWW, 2018.
10. Hoh B, Gruteser M, Xiong H, Alrabady A. Enhancing security and privacy in traffic-monitoring systems. In: IEEE pervasive computing magazine, 2018.
11. Beresford A, Stajano F. Mix zones: user privacy in location-aware services. In: Proceedings of pervasive computing, 2018.
12. Baden R, Bender A, Spring N, Bhattacharjee B, Starin D. Persona: an online social network with user defined privacy. In: Proceedings of SIGCOMM, 2018.
13. Ristenpart T, Maganis G, Krishnamurthy A, Kohno T. Privacy preserving location tracking of lost or stolen devices: cryptographic techniques and replacing trusted third parties with DHTs. In: Proceedings of USENIX security symposium, 2018.
14. Zhang S, Wang G, Bhuiyan MZA, Liu Q. A dual privacy preserving scheme in continuous location-based services. IEEE Internet Things J. 2018;5(5):4191–200.
15. Huang Z, Yan X, Lin Y, Xu Z, Lin F. A secure and efficient privacy-preserving range query scheme in location-based services. IEEE Access. 2018;6:72796–807.
16. Shahid AR, Pissinou N, Iyengar SS, Miller J, Ding Z, Lemus T. KLAP for real-world protection of location privacy. In: 2018 IEEE world congress on services, 2018.
17. Zheng L, Yue H, Li Z, Pan X, Wu M, Yang F. *k*-Anonymity location privacy algorithm based on clustering. In: IEEE June 19, 2018.
18. Zhu H, Wang F, Lu R, Liu F, Fu G, Li H. Efficient and privacy-preserving proximity detection schemes for social applications. IEEE Internet Things J. 2018;5(4):2947–57.
19. Papadopoulos S, Bakiras S, Papadias D. Nearest neighbor search with strong location privacy. In: IEEE, 2018.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.