Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Received on: 01-10-2014
Accepted on: 10-10-2014
Published on: 22-10-2014

Ravi Ranjan
Dept. of computerscience Dr .D.Y. PatilInsti. Of Engg. & Tech., Pune
Email: raviranjan9009@gmail.com
pinkeesingh15@gmail.com
priyanka171530@gmail.com
mangesh.manke1@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared

Location Privacy in Geosocial Application

Ravi Ranjan, Pinkee Singh, Priyanka Patil, Mangesh Manke
Dept. of computer science Dr .D. Y. Patil Insti. of Engg. & Tech., Pune

ABSTRACT

Now days, geosocial application have become part and parcel of our lives. But, these may be misused by someone to extract our personal info. The present paper put forth Locx that provides with improved privacy and with result quite certain. The primary thing that is done is to use secure coordinate transformation. This transformation would be used only by friends of a particular user. It allows the server to work properly and correctly without accessing the private data of the user. There are users where there is not a need for arbitrary pairs of users to be resolved. Hence, by distinguishing such location data through users social groups and further transformation can be used on location coordination. The coordinate transformations preserve distance metrics, enhancing the task of server to perform queries on transformed data. The transformation is a safe one, since the secret is the key to the data, which knows only to the users group. Here, we try to show that Locx has the capability to provide privacy and prototypes that is used in this, do the task efficiently and easily, making it near to perfect for mobile phones of the present day.

Keywords: Location privacy, security, location-based social application, efficiency.

Cite this article as:
Ravi Ranjan, Pinkee Singh, PriyankaPati, Location Privacy in Geosocial Application, Asian Engineering and Technology Innovation 02 (05); 2014; 01-04.

INTRODUCTION

In today's world, Smartphone applications have become popular among the users enhancing computing platform. A type of application is coming into line light that can be put under the category of geosocial application. Examples of this social application are local friend recommendation for dining and shopping, as well as games and collaborative network services. These are certainly good indication for these applications as is evident from mobile social networks like SCVNGR.

But, it has been noticed that these application prove disadvantages as there is a risk of losing users privacy, at present due to minimal privacy mechanism. We all know about the "places" feature of facebook which was misused by some thieves. Hence, there is a real need for stronger privacy properties in order to make it more-friendly to the users. Presently, there have been used tactics to handle this problem like 1) introducing uncertainty or errors into location data. 2) Relying on trusted servers or intermediaries to apply anonymization to users identities and private data, and 3) relying in heavy-weight cryptographic or private information retrieval (PIR) techniques. The first one needs users and application providers to give data that is not certainly leading to good enough privacy to the users. Less accuracy makes it unsatisfactory to the users & the application providers are not able to monetize the data properly. The second one depends on trusted proxies or servers that would be used by software bugs and configuration errors. Whereas, the trusted one appears quiet costly to be used on mobiles and answering queries to servers.

Therefore, we need to develop a mechanisms that would provide protection to the users privacy along with maintain the accuracy of the system. In particular, geosocial applications are to be focused. Primarily, the global visibility of the users is required to be limited. The two queries that are important for the functionality of these applications are: point queries and nearest neighbor queries (KNN). Point queries query for location data at a particular point and KNN for nearest data around a given location coordinate. We are looking forward to use these in a manner put for mobile devices at present.

In the present paper we propose LocX that helps to protect user's privacy and also maintain full accuracy in local based social application (LBSAs). There are users where there is not a need for arbitrary pairs of users to be resolved. Hence, by distinguishing such location data through users social groups and further transformation can be used on location coordination. The coordinate transformations preserve distance metrics, enhancing the task of server to perform queries on transformed data. The transformation is a safe one, since the secret is the key to the data, which knows only to the users group. Also, they are efficient, since LBSAs are least over- headed. So, these LocX lightweight built up application becomes quite fit for presently used devices.

Related work-

In this paper we introduce LocX (short for location to index mapping), a novel approach to achieve user privacy while maintaining full accuracy in location-based social applications. We want to support: 1) point query to query for data associated with a particular location, 2) circular range query to query for data associated with all locations in a certain range and 3) nearest-neighbor query to query for data associated with locations nearest to a given location.

These are the following key requirements from an ideal location-privacy service:

Strong location privacy- The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited. Location and user unlink ability. The servers hosting the services should not be able to link if two records belong to the same user, or if a given record belongs to a given user, or if a given record corresponds to a certain real-world location.

Location data privacy- The servers should not be able to view the content of data stored at a location. Flexibility to support all three queries (point, circular range, and nearest-neighbor) on location data. Efficiency in terms of computation bandwidth, and latency, to operate on mobile devices. In our proposed system, LocX, we aim to achieve all these requirements.

As per our requirements, in LocX, we do not trust any intermediaries or servers. We propose the idea of coordinate transformation in which secret angle and shift are used by the users to transform all the location coordinates they share with the servers. These secrets are known only to the friends, and therefore only the friends can retrieve and decrypt the data.

In today's systems, location data corresponding to the real-world location are stored directly on the server. But in LocX, the location is first transformed using secret angle (theta) and shift (b) as follows:

$$(X,Y)=(\cos(\text{theta})x-\sin(\text{theta})y+b,\ \sin(\text{theta})x+\cos(\text{theta})y+b)$$

Where, (x,y) are real coordinate of a location and (X,Y) are transformed coordinate of that location.

Location data are then encrypted using secret symmetric key. Then, the user generates a random index (i) using his random number generator and encrypt it with his symmetric key. In LocX, we split the mapping between the location

and its data into two pairs: A mapping from the transformed location to an encrypted index (known as L2I), and a mapping from the index to the encrypted location data (known as I2D). We refer to the server storing L2Is as index server and the server storing I2Ds as the data server. User store and retrieve the L2Is via untrusted proxies. Then, the transformed location is decoupled from the encrypted data using random index i via two servers as follows: 1) an L2I, which stores encrypted random index under the transformed location coordinate and 2) an I2D, which stores the encrypted location data under the random index i. As the user shares these secrets to the friends, only the friends can retrieve and decrypt the data.

Here we describe how LocX's meets all of our requirements:

Defending against an attacker with access to data on the servers-The data stored on both servers do not reveal any information about their locations to the attacker. The L2Is on the index server contain transformed coordinates and the data on the data server are all encrypted. As a result, an attacker with access to just the data on these servers cannot deanonymize the data to associate users with their locations.

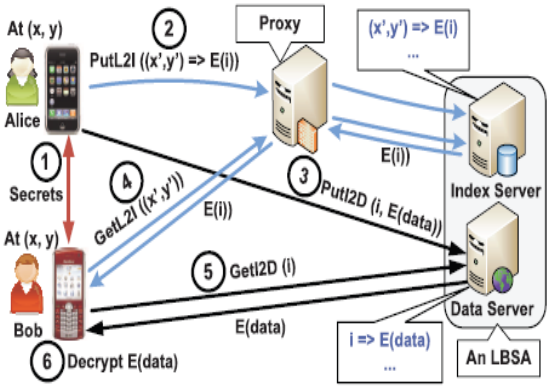

Fig. Design of LocX

L2I – mapping from location to an encrypted index

I2D - mapping from index to an encrypted location data .

Location privacy during server access- Even the attacker with access to monitor both servers cannot link accesses to the index and the data server because the indices stored on the index server are encrypted, but the indices are not encrypted on the data server. Only the users know how to decrypt the encrypted indices. Without the decryption keys, the attacker cannot link these records to figure out even the transformed location of the users accessing the servers.

Location data unlinkability- The I2Ds are encrypted and the users access them only via indices. Hence, users cannot be linked to any locations. The indices stored or accessed by a user are random numbers. The data server can link together the indices accessed by the same user, but this does not help the servers link the user to any locations. Finally, the users store and retrieve L2Is on the index server via proxies, so servers cannot link different transformed locations to the same user. Together, these provide location unlink ability.

Literature Survey-

No.	Paper name	Publication	Year	Merits	Demerit
1.	Location Anonymity in mobile geosocial network	IEEE	2013	Gives nearby friend alert	"Nearby friend alert" in mobile geosocial networks requires addressing privacy issues
2.	Providing source location privacy in WSN	IEEE	2013	Wireless sensor network is low cost device. Used to monitor movements of PANDA in National Park.	SLP requires that flow of message does not give away location of source node. In fact confidentiality of message is a part of another privacy category.

3.	Foursquare	IEEE	2008	Facilitate communication & interaction among who may be well known to one another or unknown to one another	It is not trust E-verified Do not provide privacy, data shown publicallys.
4.	Location related privacy in Geo-social networks	ACM Press	2010	Privacy of location,absence,co-location & identity privacy are provided	Requires more expressive formal model that's applicable to all of addressed scenarios.

Acknowledgement-

With immense pleasure, we are presenting this paper as part of the curriculum of B.E. Computer Engineering. We wish to thank all the people who gave us an unending support right from the stage the idea was conceived. We express our sincere and profound thanks to Mr. Mangesh Manke (Project Guide and Head of Department), Mrs. SharmilaChopade(Project Coordinator) and all the teachers. We are also thankful to all our classmates who helped us in the preparation of this paper. We also acknowledge the research work done by all researchers in this field.

Future Work-

In future user's privacy location in LocX is not so easy, it is very expensive. Hence LocX improves location privacy. This LocX runs efficiently on constrained mobile phones. LocX add little bit computational and communication overheads to the existing systems. Hence LocX takes big steps towards location privacy for emerging large class of geosocial application.

REFERENCES

1. H. Hu, J. Xu, C. Ren, and B. Choi, "Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), 2011.
2. W.K. Wong, D.W.-L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN Computation on Encrypted Databases," Proc. SIGMOD Int'l Conf. Management (SIGMOD '09), 2009.
3. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An Online Social Network with User Defined Privacy," Proc. ACM SIGCOMM Conf. Data Comm., 2009.
4. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.
5. M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007.
6. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing Magazine, vol. 5, no. 4, pp. 38-46, Oct. 2006.
7. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data, 2008.
8. S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.
9. A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011.