Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Received on: 01-12-2014
Accepted on: 10-12-2014
Published on: 22-12-2014

Reena Gandhi, Charushila Kapde, Priyanka Kumbhar, Bindu Pandit,
Prof. S. S. Sambare
Dept. of computer engineering, PCCOE, Nigdi, Pune 44
reenagandhi67@gmail.com
kapadecharu@gmail.com
priyanka6605@gmail.com
bindupandit63@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared

Enhance Recommendation by Providing Location Privacy in GeoSocial Application

Reena Gandhi, Charushila Kapde, Priyanka Kumbhar, Bindu Pandit, Prof. S. S. Sambare
Dept. of computer engineering, PCCOE, Nigdi, Pune 44

ABSTRACT

In today's world, there are many geosocial applications which are based on large extent. But the location privacy provided is very inadequate. In this paper, we are using LocX, which is a novel alternative for improving location privacy without adding uncertainty or relying on strong assumptions. User shares their secrets which get stored on server in encrypted format by using transformations. Recommender can access the users location and data by using symmetric key. LocX provides privacy with little performance overhead making it useful for today's mobile devices.

Keywords: LocX, Location based service area, security, efficiency.

Cite this article as:
Reena Gandhi, Charushila Kapde, Priyanka Kumbhar, Bindu Pandit, Prof. S. S. Sambare, Enhance Recommendation by Providing Location Privacy in GeoSocial Application. Asian Journal of Engineering and Technology Innovation 02 (05); 2014; 38-42.

INTRODUCTION

It is a well-known fact that the progress of personal communication devices leads to serious concerns about location privacy issues. As a response to these issues, many Location-Privacy Protection Mechanisms (LPPMs) have been proposed during the last decade. The assessment and comparison remains problematic because of the absence of a systematic method to quantify the issues. In particular, the assumptions about the attacker's model do not tend to be complete, with the risk of a possibly wrong estimation of the users' location privacy.

Modern communications mean most individuals today walk around with a beacon that transmits user's location. Mobile phones register to a nearby tower as the owner moves through space and the phone company can collect that data in real time or retrospectively to physically place the phone with varying degrees of accuracy. There are many companies that can also determine the owner of every handset within range of a specific tower. GPS enabled phones enable far more precise location placement[3].

Many cars now have GPS devices installed some of which transmit the vehicle's location to a centralized service. As the devices are available at cheaper cost and smaller law enforcement agencies can more easily attach GPS trackers to cars and individuals enabling precise round-the-clock surveillance. Location-based services including maps of nearby restaurants friend finders and other social networks collect location data as part of providing the service or for contextual advertising.

LocX (short for location to index mapping), is a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here onward). Many services do not need to resolve distance-based queries between arbitrary pairs of users; it is only between friends interested in each other's locations and data. Thus, partition can be done on location data based on users' social groups. After which transformations are perform on the location coordinates before storing them on untrusted servers. As user knows the transformation keys of all user's friends, it allows transforming query into the virtual coordinate system that user's friends uses. Coordinate transformations preserve distance metrics, thereby allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. The transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is known only to the members of the social group. These transformations are efficient, and incur minimal overhead on the LBSAs. The applications built on LocX lightweight and suitable for running on today's mobile devices.

2. SYSTEM FEATURES

The key features of Locx system are:

1. Strong location privacy-server is not able to trace the history of user's location.
2. Location and user unlink ability. If two records are found of the same user at different places , then server should not be able to link user with data.
3. Location data privacy. The servers should not be able to fetch the data stored at particular location.
4. Flexibility to support different types of queries like point, circular range, and nearest-neighbor queries on location data. .
5. System provides efficiency in terms of computation, bandwidth, and latency [1].

3. related work

No.	Paper name	Description	
1.	Location Anonymity in mobile geosocial network IEEE 2013	Nearby friends alert are given. "Nearby friends get alert " in mobile 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 publically.	
4.	Location related privacy in Geo-social networks ACM Press 2010	Privacy of location, absence, co-location & Identity privacy is provided. Requires more expressive formal model that's applicable to all of addressed scenarios.	

Locx system

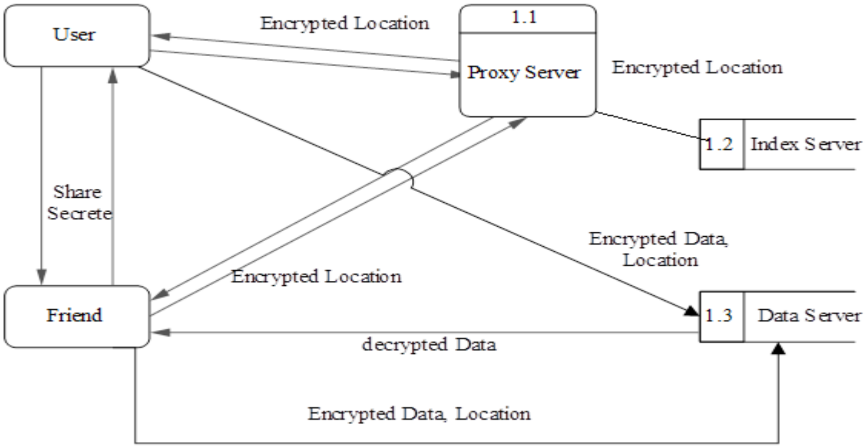

Fig. System architecture

In this design,

1) User and users' friend exchange their secrets
2) User stores his review of the restaurant (at(x,y)) on the server under transformed coordinates.
3) Friend later visits the restaurant and queries for the reviews on transformed coordinates
4) Decrypts the reviews obtained.

Modules

1. Network Formation
2. Data Storage
3. Data Retrieval
4. Location Data Access

Module Description

1. Network Formation

In this module the network formed for preserving location privacy. The network contains proxy, data server, index server and number of mobile users.

2. Data Storage

When a user generates the location data corresponding to a location (x, y), she/he uses her/his secrets to decouple it into a L2I and an I2D.

Storing L2I on the index server

The user transforms real-world coordinate to a virtual coordinate using secret rotation angle and secret shift available to the user. This transformation preserves the distances between points. The circular range and nearest-neighbor queries for a friend's location data can be processed in the same way on transformed coordinates as on real-world coordinates. The user then generates a random index (i) using random number generator and encrypts it with her symmetric key.

Storing I2Ds on the data server

The user can directly store I2Ds (location data) on the data server. This is secure because the data server only sees the index stored by the user and the corresponding encrypted blob of data. For example, a location-based video or photo sharing service might share multiple MBs of data at each location.

3. Data Retrieval

In this module the users add noise to the query when provide the privacy while querying the index server. By adding noise, coupled with routing the index server queries via proxies (just like the way they were stored), provides strong location privacy during querying. The queries only contain a list of points in the transformed coordinate space, without containing any user identifier or actual location information.

4. Location Data Access

When a user accesses her friends' data by transforming her own location to different points in the transformed space and sending them in a query, a malicious index server transformed coordinates that map to the same real-world location (which is the user's current location). Constraints in querying the index server, Impact of malicious proxies and improving privacy using noisy queries.

Following are the Five Types of user classes with characteristics:

- **Up-to-Date:** These people stay current with the news, weather and events at all times. These people like to be informed and others look to them as beacons of information. They always use their mobile phone as a resource to keep them connected with real-time information about the world around them [1].
- **Social and Curious:** These people are sometimes described as connectors because they enjoy bringing others together making plans and outings too. They use their mobile phones to stay connected to the people they care about [4].
- **Busy and Productive:** This group of people is very concerned with all information related to their own personal efficiency and their ability to cope with a busy schedule. They prefer application which is more portable, accessible than using traditional computers. They are interested in applications that can help them manage their multiple priorities and meet the demands of their busy day.
- **Latest and Greatest:** These people want to be the first to try any application, even if there is no guarantee that they will be satisfied with it. They always prefer to use the latest technologies and applications and to be a part of the latest social networks and communities. Their friends always look to them for reviews and recommendations of new technologies.
- **Just the Basics:** This group of people is only interested for the applications that make life easier. They are not impressed by the latest technology or the marketing appeals of most applications. They do not adopt easily and they look to reviews and recommendations to find the tools and applications that they want to use.

ASSUMPTIONS AND DEPENDENCIES

Location coordinates refer to the longitude, latitude pairs which are associated with real-world locations. A pair of coordinates is returned from a GPS, associating data with a location. Location data or location information refers to such data associated with a location. For example, when reviews (referral point details) are written for a given restaurant, these reviews are the location data associated with the restaurant's location coordinates.

The companies that provide LBSA services manage the servers. The data is stored by user on the servers to obtain the service. These companies are responsible for reliably storing this data, and providing access to all the data that user should have access to. The companies can get incentives for displaying ads, or charging some usage fees of user. In the attacker model, the attacker has access to the LBSA servers [7]. This attacker can be an employee of the company running the service or an outsider that compromises the servers. The attacker might even be an oppressive regime or a government that obtains data from the providers via subpoenas.

As a result, in this model the attacker can access all the data which is stored on the servers, and can also monitor pieces of information which is been accessed by the user on the servers. Our goal is to design a system that will preserve the location privacy of users.

The attacker does not perform any attacks on the consistency or integrity of data on the servers, but aims only to gain access to users' location information. Finally, like all prior social systems. The friends of a user are trusted and do not collude with the servers in breaking the user's privacy.

Mathematical Equation

Let S be the system,

S = {M, h, Q, b}

Where,

M=Number of queries.

h= Number of friends.

Q= Secret Angle.

b= Shift

Transformed coordinate = (xij,yij) for all m queries.

$Eq^n= (2n_1+ 2n_2 + \dots\dots\dots+ 2n_m)$ (index server)

So, there are 2 equations for each requested friend at one location to solve 2m unknown real co-ordinates (x_j,y_j) and 2n unknown friend's secrets (Θ_i,b_i), where 1<=j<=m, 1<=i<=n

$\cos\Theta_i.x_1 - \mathrm{Sin}\ \Theta_i.y_1 +b_i = x_{i1}$

$\cos\Theta_i.x_1 + \mathrm{Sin}\ \Theta_i.y_1 +b_i = y_{i1.}$

$\cos\Theta_i.x_m - \mathrm{Sin}\ \Theta_i.y_m +b_i = x_{im}$

$\cos\Theta_i.x_m + \mathrm{Sin}\ \Theta_i.y_m +b_i = y_{im}$

So, Total variable = 2m + 2n

1. Number of unknowns for all = $n_1 + n_2+\dots\dots\dots+n_m> m+n$

2. Authentication= $n_1 + n_2 + \ldots\ldots\ldots + n_m < m+n$
3. All n friends data, $mn < m+n$

4. CONCLUSION

Hence we conclude that the description of prototype implementation, design and LocX evaluation which is a system for building location-based social applications (LBSAs) while preserving user location privacy. LocX provides location privacy for registered users without injecting insecurity or errors into the system, and does not rely on any trusted servers or components.LocX takes a novel and is a new approach to provide users location privacy while maintaining overall efficiency of a system, by leveraging the social data-sharing property of the target applications. In LocX, user can efficiently transform and store all their locations shared with the server and encrypt all location data stored on the server using reasonably priced symmetric keys. Only friends having right keys are able to query and decrypt a user's data. LocX introduces several mechanisms to achieve both privacy and efficiency. It also analyzes their privacy properties.

Using evaluation, based on both synthetic and real-world
LBSA traces, LocX adds little computational and communication overhead to existing systems. LocX
prototype runs efficiently on mobile phones. Overall, we conclude that LocX takes a big step towards making location privacy practical for a large class of emerging geo-social applications.

REFERENCES

1. Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer,Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao, "Preserving Location Privacy in Geo-Social Applications", Department of Computer Science, UC Santa Barbara IEEE 2012.
2. "SCVNGR," http://www.scvngr.com, 2013
3. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011
4. 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.
5. 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.
6. 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.