ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Survey on Preserving Location Privacy in Geosocial Applications

Manu. P. Krishna, Jose Hormese

M.Tech, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India

Assoc.Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India

ABSTRACT: By tremendous improvement of pinpoint localization, more number of geo-social applications are used by millions, which gives an opportunity to interact, also sharing locations to unknown. However today's geo-social application have many privacy issues, which can easily misused by an expert even a well known person. LocX is a latest technique used for providing security in geosocial application. In LocX working scenario, Location coordinates are transformed before updating to server. User must exchange their secret key prior to location sharing , . Medium of sharing key is via mail or messages. This mechanism is not suited for high end geosocial applications. One user can hold the secret key of his N friends. LocX is efficient but not a novel method, for reduce the complexity a new technique for Location privacy is introduced ,using attribute based encryption instead of sharing secret keys. By adopting this way, it provides performance overhead and ease of use.

KEYWORDS : Location privacy, security, location-based social applications,coordinate transformation

I. INTRODUCTION

Smartphones have provided a huge boost to the popularity of geosocial applications, which facilitate social interaction between users geographically close to each other. However, today's geosocial applications raise privacy concerns due to application providers storing large amounts of information about users (e.g., profile information) and locations (e.g., users present at a location). Android are quickly becoming the dominant computing platform for today's user applications Early location based applications enabled users to retrieve content relevant to their current location (e.g., points of interests (POIs) [1]).

Today many applications fully exploit all the features powered by Gps service. Millions of peoples were used facebook and foursquare, it gives immense options for tagging, sharing current location of user. Many peoples are not known the risk factors , today's geosocial applications raise privacy concerns due to application providers storing large amounts of information about users. Strong privacy protection demands for better security. Location privacy by attribute to design mechanisms that efficiently protect user privacy without sacrificing the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers [8].

II. PROBLEM STATEMENT

Geosocial applications and user rate will be raised day by day. Utilize all funtionality available in a typical application is possible only, if there is no privacy and security issues. Location system privacy by attribute based encryption is more acceptable by comparing to existing system. Locx is one of an existing technique used for protecting coordinates from unauthorized access. But the methods adopt for locx system is bit difficult. In existing system, user need to share secret key through a secure medium. It is not a novel approach, millions of peoples used this geosocial application. By adopting this existing technology one user contain his N friend secret key. It also affect the performance of entire system [1].

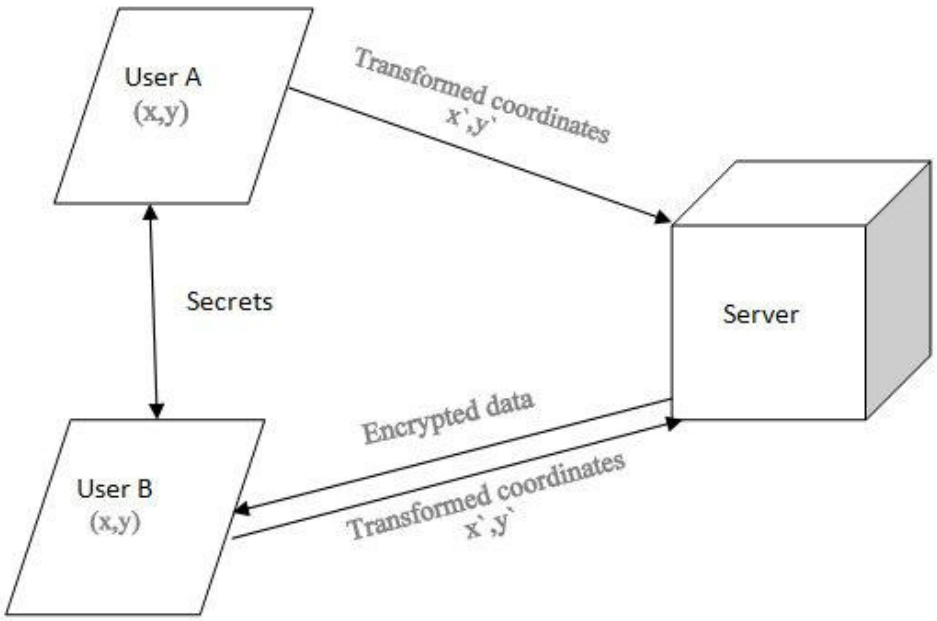
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

III. LOCX WORKING PRINCIPLE



- User A and B exchange their secrets
- User A store the review of the place at (x,y).Transformed and store
- User B later visit the place and queries for the review on transformed coordinates.
- Decrypts the review obtained.

IV. PRIVACY PRESERVING TECHNIQUES

A. Adaptive-Interval Cloaking :

The key idea underlying this algorithm is that a given degree of anonymity can be maintained in any location regardless of population density by decreasing the ac curacy of the revealed spatial data. [5]To this end, the algorithm chooses a sufficiently large area, so that enough other subjects inhabit the area to satisfy the anonymity constraint The desired degree of anonymity is specified by the parameter k_{min}, the minimum acceptable anonymity set size. Furthermore, the algorithm takes as inputs the current position of the requester, the coordinates of the area covered by the anonymity server, and the current positions of all other vehicles/subjects in the area[4].

An orthogonal approach to spatial cloaking is temporal cloaking. This method can reveal spatial coordinates with more accuracy, while reducing the accuracy in time. The key idea is to delay the request until k_{min} vehicles have visited the area chosen for the requestor. The spatial cloaking algorithm is modified to take an additional spatial resolution parameter as input. It then determines the monitoring area by dividing the space until the specfield resolution is reached. The algorithm monitors vehicle movements across this area. When k_{min} different vehicles have visited the area, a time interval [t1,t2] is computed as: t2 is set to the current time, and t1 is set to the time of request minus a random cloaking factor. The area and the time interval are then returned[10].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

B. Anonymizing Location Information :

The mobile nodes communicate with external services through a central anonymity server that is part of the trusted computing base. In an initialization phase, the nodes will set up an authenticated and encrypted connection with the anonymity server. When a mobile node sends position and time information to an external service, the anonymity server decrypts the message, removes any identifiers such as network addresses, and perturbs the position data according to the following cloaking algorithms to reduce the reidentification risk. [5]Moreover, the anonymity server acts as a mix router, which randomly reorders messages from several mobile nodes, to prevent an adversary from linking ingoing and outgoing messages at the anonymity server. Finally, the anonymity server forwards the message to the external service

C. Location Transformation :

Transforming IDs is not enough to provide location privacy for users because some locations (e.g. homes) are strongly associated with user IDs and may thus cause information leak [2]. Location transformation, which is a crucial feature adopted for privacy. The main challenge in the development of suitable functions for location transformation is to keep the relative distance in each sub-dataset (the dataset obtained from the same agent) unaltered by the transformation in order to support location based services (e.g. nearest neighbor queries). [1]Possible transformation functions include scaling, rotating, translation, and their combinations.

D. Query Transformation :

A range query retrieves all objects the location of which falls within the circular range at a given query timestamp. Due to the multiple transformation on the users' positions, a query has to handle data from different transformations.[5] [6] One solution is to transform the query using all transformation functions, and then execute multiple queries , this is not efficient and may disclose the relationship among transformation functions. Such situations we can use super query, which covers all queries after multiple transformations. It guarantees that the radius of the super range query is at most λ larger than that of any transformed query. It is true that the super query may incur some overhead due to the search of a larger space compared to the query transformed by any one of the transformation functions.

Along transform the coordinates it is also necessary to keep its distance preserving value. For that the transformation must be accurate. To transform a real world coordinate into virtual coordinate, secret shift (b_u) and rotation angle is Θ_u used [2]

$$x`,y`=(\cos\Theta_u x - \sin\Theta_u + b_u , \sin\Theta_u x + \cos\Theta_u y + b_u).$$

E. Personalized Location k-anonymity

The Location Based System(LBS) system consists of mobile nodes, a wireless network, anonymity servers, and LBS servers. Location information is typically determined by a location in formation source, such as GPS receiver in a vehicle. Location information includes temporal information (when the subject was present at the location) in addition to spatial information. Mobile nodes communicate with third party LBS providers through one or a collection of anonymity servers located at trusted computing bases. The mobile nodes establish communication with an anonymity server through an authenticated and encrypted connection. Each message destined to an LBS provider contains location information of the mobile node, a timestamp, in addition to service specific information.[6] [12] Upon receiving a message from a mobile node, the anonymity server decrypts the message and removes any identifiers, such as IP addresses, and perturbs the location information through spatio-temporal cloaking, and then for location information includes temporal information (when the subject was present at the location) in addition to spatial information. Mobile nodes communicate with third party LBS providers through one or a collection of anonymity servers located at trusted computing bases.[6] The mobile nodes establish communication with an anonymity server through an authenticated and encrypted connection. Each message destined to an LBS provider contains location information of the mobile node, a timestamp, in addition to service specific information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Upon receiving a message from a mobile node, the anonymity server decrypts the message and removes any identifiers, such as IP addresses, and perturbs the location information through spatio-temporal cloaking, and then for The main task of a location anonymity server is to transform each message received from mobile nodes into a new message that can be safely (k anonymously) forwarded to the LBS provider. The key idea underlying the location k-anonymity model is two-fold. First, a given degree of location anonymity can be maintained, regardless of population density, by decreasing the location accuracy through enlarging the exposed spatial area, such that there are other k − 1 mobile nodes present in the same spatial area.

F. K Nearest Neighbor Query :

Given a query object with position (qx, qy), the k nearest neighbor query (kNN query) retrieves k objects for which no other objects are nearer to the query object at a given query timestamp. One way to compute this kind of query is to transform the position of the query object using all the functions in the agent's transformation table.[9] And the server needs to consider kNN[5] for each transformed query position. For simplicity, compute the kNN query by iteratively performing range queries with an incrementally expanded search region until k answers are obtained. Like the range query, a kNN query also needs to be sent to all agents. The main difference is that each agent needs to convert the kNN query to a range query first. Then the agent transforms the range query and the expansion parameter r_q, and sends them to the server.[10] The server will keep processing the range query q with the radius extended by rq each time, and return the query result to the agent once it obtains k qualified answers. Finally, each agent computes the correct distance, and sends the distance along with the user IDs to the user that issued the query. The user then combines these to find his true k nearest neighbors.

V. ATTRIBUTE BASED ENCRYPTION

In a distributed collaborative system, it is often convenient for the members to communicate with the others in the system using attributes that describe their roles or responsibilities. These attributes are highly desirable if the members join/leave the system dynamically. Consider an Internet forum where the members are organized into user groups based on the members' skills or privileges. It is a natural requirement that the members of a user group should be able to establish secure communication with the other members belonging to particular user groups. The communication in these forums is generally carried out through initiating a thread or by posting messages within an existing thread.

To enable authentic and confidential communication, the forum administrator may specify an access policy with the user groups being attributes. Obviously, only the members of the forum whose attributes (e.g. membership to user groups) satisfy the policy should be able to have read and/or write access to the thread. There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center,dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submit

Ciphertexts are associated with sets of attributes, whereas user secret keys are associated with policies. As we have discussed, this set ting has a number of natural applications. Another possi bility is to have the reverse situation: user keys are associated with sets of attributes, whereas ciphertexts are associated with policies. We call such systems Ciphertext-Policy

Attribute-Based Encryption (CP-ABE) systems.CP-ABE systems that allow for complex policies (like those considered here) would have a number of applications. An important example is a kind of sophisticated Broadcast Encryption, where users are described by (and therefore associated with) various attributes. Then, one could create a ciphertext that can be opened only if the attributes of a user match a policy [16]

VI. CONCLUSION AND FUTURE WORK

This survey paper presented an overview on the privacy feauture to geosocial applications. But the system complexity is too high by sharing secret keys among all user.Instead of sharing secret key among users,encrpty and decrypt by using this attribute based.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

REFERENCES

1. Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, "Preserving Location Privacy in Geosocial Applications"Proc IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014
2. D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position Transformation: A Location Privacy Protection Method for Moving Objects," Proc. Int'l Workshop Security Privacy GIS LBS, 2008.
3. A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004
4. B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005.
5. M. Gruteser and D. Grunwald, "Anonymous Usage of Location Based Services through Spatial and Temporal Cloaking," Proc. First Int'l Conf. Mobile Systems, Applications Services, 2003.
6. B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.
7. "Police: Thieves Robbed Homes Based on Facebook, Social Media
Sites," WMUR News, http://www.wmur.com/r/24943582/detail.html, Sept. 2010.
8. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second Generation Onion Router," Proc. 13th Conf. USENIX Security Symp., 2004.
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
10. A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, 2007
11. "Police: Thieves Robbed Homes Based on Facebook, Social MediaSites," WMUR News, http://www.wmur.com/r/24943582/ detail.html, Sept. 2010.
12. 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
13. A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004
14. "Privoxy Web Proxy," http://www.privoxy.org, 2012.
15. 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
16. Vipul Goyal, Omkant Pandey, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data",

BIOGRAPHY

Manu P Krishna is a MTECH Student in CSE, Marian Engineering college kazhakuttom, Thiruvananthapuram

Mr. Jose Hormese is working as Associate Professor at Department of CSE, Marian Engineering college kazhakuttom, Thiruvananthapuram