International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 2: February 2016, pp 40-42. www.aetsjournal.com ISSN (Online) : 2394-6237

Protecting User Identity in Geo-Social ApplicationsUsing Coordinate Transformations

P.kruthika , T.sounderrajan

Abstract— Now a days people mostly depend on the geo-social applications which is a location based service which serves the user by providing recommendations about the neighbor places from their vicinity. Using such applications, the user interacts with their surroundings to know about their search locations and to share their reviews. Due to the lack of protection to their location identity the user's location information is misused by the hackers and other unwanted users to get access to the personal information such economic gain physical stalking etc. Location to index mapping is a technique that provides the security to user identity by preserving coordinate transformation to the location data that shared with the servers. It is made suitable to implement in the mobile devices.

Key words: Geo-social applications, Location security, Location transformations, security.

I. INTRODUCTION

Millions of people use the smartphones for the attractive applications which is provided by the Android and Apple iTunes computing platforms. Among those applications geo-social applications are highly used, which act as an interface to interact with the surroundings to know about the best recommendations for shopping, banking and dinning [1], [2].

This kind of location based applications is associated with several security issues in sharing the location identity and the information associated with it. The Geo-social applications such as scvngr, Loopt etc., work by using the fine-grain and time stamping information. Since there is least privacy protection in these services, the information about the users can be misused by the hackers.

So the application which is meant to provide services to regarding the location of the user should be provided with strong security policies.

II. RESEARCH OBJECTIVE

There are several solutions available for providing security to the location data of the user such as, using the spatial and temporal cloaking [3],in which three kind of translators are used. First is the policy translator, defines the privacy preferences. Second is the service translator, defines the cloaking agent according to the preference mentioned by the policy translator. Third is the result translator, this provides the service to user regarding their search.

Another solution is that kNN queries are splitted into number of database blocks [4]. These queries are retrieved using secure hardware Private information retrieval method. This helps to hide the block in which the queries are stored from the location based applications.

Some other approaches are introducing the anonymous routing system such as Tor [5] for sending the queries but this is not always efficient for the LBS (Location Based Services) The Tor is used to secure the anonymity while using the internet. It consist of a software to use the internet and a volunteer network to make use of that software.

Using Click Cloak Algorithm [6] to provide high quality personalized location K-anonymity. Itreduces the known location privacy threats before forwarding the request to LBS providers.

III. RELATED WORK

The previous solutions mainly concentrates on three approachesto provide privacy to the user identity and their related information, which is based on introducing noise into the data, depending on the intermediate servers, and using cryptographic technologies.

A. Introducing error into the data

In this technique some error is introduced along with the user identity information[7], [8]which makes the hackers difficult to identify the valid details.

Injecting the noise into the data is a risky solution, because the private data can be exposed by the malicious administrators.

However, this approach pitfall due to loss of accuracy in the result given to the users. And it also difficult for the application providers to monitor the user data.

B. Depending on the intermediate servers

The user details were send via the proxies or other intermediate servers that transform the original details [9], [10] of the user which cannot be identified by the unwanted users or hackers.

This method providing protection to user information suffer because of hacking the intermediate servers to which the user's actual details are shared. In this by attacking the intermediate proxy servers the details can be accessed by the hackers.

P.kruthika, PG Scholar, KSR Institute for Engineering and Technology, Dept of CSE (Email : kruthika9293@gmail.com)

T.sounderrajan, Assistant Professor, KSR Institute for Engineering and Technology, Dept of CSE (Email : tsounderrajan@gmail.com)

C. Using cryptographic techniques

The cryptographic techniques provide the privacy to the information of the user.The Private Information Retrieval (PIR) [11], [12], [13], [14] method is method to provide protection to the user information.

But these techniques are not suitable for the mobile devices which often in mobility. These are considered as heavy weight cryptographic techniques that cost high to implement in the mobile devices.

IV. PROPOSED SYSTEM

Main concept to implement in the proposed system is that it has to provide privacy protection to hide the location details about the user without inventing heavyweight cryptographic methodology or other existing solutions which degrades the performance and the quality of the services provided to the customer.

For this purpose, Location to index mapping (LocX) is introduced which efficiently provides security in location based applications.LocX does not introduce uncertainity into the data or does not depend on the intermediate systems to provide security.

A. Scenarios in location based applications

First scenario:

Two friends at different location in a vicinityshares their recommendations about the places for dinning, hospitals or some other details. Another friend who searches for the location details in same vicinity should able to make use of the information that is already posted by his friend.

Second Scenario:

A person in a location needs to query an application to know about the places and to know the better option for their need from the user surrounding.

B. System Requirements:

Based on the scenarios of the location based applications following are the requirements derived.

- Strong location privacy. The servers which process the queries of the user should not know about the locations the user had so far visited.
- Location and user unlinkbility. The servers providing the services to the users should not able to locate the real world location of the user and also they should not reach the user by using the similarities of the search queries.
- Location data privacy. The servers and also hackers should not able to know about the data stored in the location.
- Efficient support for the point queries and the nearest neighbor queries.

V.SYSTEM DESGIN

A. overview ofLocX

In the Location to index mapping method the user identity and the data with it is separated and stored in different servers. The user identity is stored in the index server and the data associated with it stored in the data server.

Initially the user identity is transformed according to its location coordinates in the mobile device itself and then stored in the index server via the proxy server. Here the proxies also know only about the transformed values not the original identity information.

Then the data separated from the identity information is encrypted and stored in the data server the user with the right key can decrypt the message. The key is shared with the user friend list prior via face to face contact, through mail or phone calls.

B. Architecture

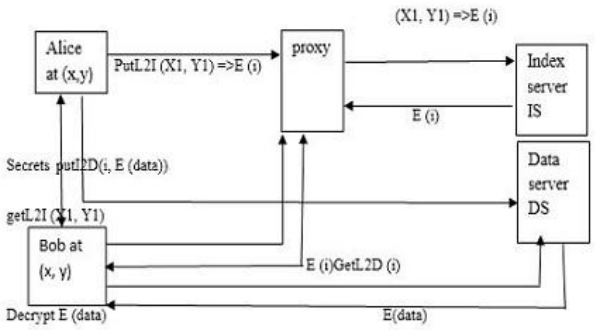

Fig. 1 Design of LocX

Initially the secret key is shared between the friends, there can be N number of friends in a vicinity. Then the information that is shared with the servers and friends are divided into identity information, which stores the location data about the user and the data associated with the user identity.

The location information (x,y) is converted to (x',y') and stored in the index server (L2I) Location to Index server via proxy server. The data associated with it is encrypted and stored in the data server (I2D) Index to Data server. The person with the correct key can able to decrypt the encrypted data E (data) is stored in the data server.

The index server can also able to see only the converted location not the real world identity of the user. And the mapping of the data in the data server with its location identity in the index task is also a challenging task for the hackers to get access to the user's location information.

VI. EVALUATION

A. Implementation

The LocX is implemented in java by using AES with 128 bits keys for encryption and decryption purpose. The nearest neighbor queries are processed using the R* tree package from the HKUST [15].

The LocX performance is measured both in the desktop and in mobile phones. The same code is used for the mobile phones but there require slight changes to support for some of the missing android libraries.

B. Experimental Setup

The overhead occur is evaluated, by comparingLocX location to data server L2D with random tags. There is no encryption or decryption in L2D i.e., L2D is a plain-text. The calculation is performed by measuring the communication cost, clients processing time, the query completion time this includes the network latency, and the server processing time

The analysis is taken under the categories of performance of the location put and the query performance when increase in the # puts.

Performance of the location put. A put in the LocX method does not have any client processing time because there is no need of decrypting in L2D. The encrypted data stored in the data server have the client processing time and possess only low overhead that is not even noticed by the application users. The average message size is 84.5 in L2D, it is increased to 140 in LocX. In k-Anonymity the message size is higher compared to LocX due to cloaking spatial region in the message.

Query performance when increase in the # puts. The query processing is compared between LocX, K-anonymity, L2D for point query and the nearest neighbor query. The message size is fixed 140 as maximum in synthetic data set and location put is varied from 20 to 100 per client. When the location put increases the query need to processed get increased.The query processing in LocX, takes less time compared to the K-Anonymity and LocX with no tags.

VII. CONCLUSION

LocX is a method which provides the privacy protection for user information in location based applications with affecting the quality of the services given to the user. This method efficiently transforms all the location identities that is accessed by the servers and also encrypt the data associated with it. This technique is analyzed in both the synthetic data and the real-world LBSA traces.

LocX uses light weighted cryptographic technique that makes it to run efficiently in the mobile devices. However the LocX technique have little computational and communication overhead this can be enhanced in the future considerations.

REFERENCES

[1] M. Hendrickson, "The state of location-based social networking," 2008.
[2] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in *Proc. of SenSys*, 2008.
[3] M. Gruteser and D. Grunwald, "Anonymous usage of location-basedservices through spatial and temporal cloaking," in *Proc. of Mobisys*, 2003.
[4] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest NeighborSearch with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.
[5] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," Proc. 13th Conf. USENIX Security Symp., 2004.
[6] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005.
[7] 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.
[8] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005.
[9] T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy inWirelessLans," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.
[10] 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.
[11] 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.
[12] 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.
[13] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011.
[14] Zhong, I. Goldberg, and U. Hengartner, "Louis Lester andPierre: Three Protocols for Location Privacy," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, 2007.
[15] D. P. group, "R-tree java implementation, "http://www.rtreeportal. org/code/Rstar-java.zip.
[16] Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Proc.of SSTD*, 2007.
[17] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous locationbased queries in distributed mobile systems," in *Proc. OfWWW*, 2007.
[18] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. of Pervasive Computing*, 2009.
[19] Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," in *IEEEPervasive Computing Magazine*, 2006.Hoh *et al*., "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proc. of CCS*, 2007.
[20] J. Krumm, "Inference attacks on location tracks," in *Proc. Of Pervasive Computing*, 2007.
[21] A. Beresford and F. Stajano, "Mix zones: User privacy in locationaware services," in *Proc. of Pervasive Computing*, 2004.
[22] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services," in *Proc. of ICDE*, 2008.
[23] Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position transformation: a location privacy protection method for moving objects," in *Proc. Of Security and Privacy in GIS and LBS*, 2008.
[24] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in *SSTD*, 2007, pp. 258–275.
[25] O. Turgay, T. B. Pedersen, Y. Saygin, E. Savas, and A. Levi, "Disclosure risks of distance preserving data transformations," in *Proc. of SSDBM*, 2008.
[26] S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized Privacy preserving computation of users' proximity," in *Proc. OfSDM*, 2009.
[27] S. Mascetti, C. Bettini, D. Freni, X. S. Wang, and S. Jajodia, "Privacyaware proximity based services," in *Proc. of MDM*, 2009.
[28] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *USENIX Security Symposium*, 2004.
[29] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in *ICDE*, 2011.
[30] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *SIGMOD Conference*, 2009.