International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 28287-28294

http://www.ripublication.com

An Efficient Privacy Preserving Mechanism In Geo-Social Applications

S. Deepika
M.Tech 2nd year, Dept. of CSE, SVEC
Tirupati, A.P, siddilingamdeepika@gmail.com
D.Ganesh
Assistant Professor, Dept. of CSE, SVEC
Tirupati, A.P, dgani05@gmail.com

Abstract

Geo-social applications are most commonly used in which different communities integrate together with their surrounding environment through their friends and their recommendations. Such systems can be misused easily through various attacks. Hence providing privacy to the geo-social applications became main issue. The existed system, *LocX*, that provides significant improving location privacy by not adding uncertainty into the query results or rely on strong assumptions about security of the server. Here user send message to other user is of bigger size, so that the expense of the server database increases on existing system. Therefore compression algorithm is proposed to compress the message by that the message retrieval time reduces than the existed system. This method provides privacy and improves the performance of geo-social applications.

Keywords: Location privacy, Security, Location based services, Geo-social applications, Location transformation, and efficiency.

Introduction

Online Social Networks (OSNs) are virtual integration center points, permitting clients to keep up contact with relations. Online Social Networks (OSNs) have encountered huge development lately and turn into a true entrance for countless Internet clients. These OSNs offer alluring means for advanced social co-operations and data offering additionally raise various security and protection issues by uncovering the client's information like age, sex, contact, inclinations and their current announcements. With the appearance of geo-social systems like Yelp (GSNs) and Foursquare give fine grained area data about the users, the spots went to, registration performed. This data gives the GSN Applications a route for giving customized

proposals and area based focused by the site owner prompting the site owner's complex increment in business. Geo-social systems (GSNs) are a famous expansion of the developing online social networking systems.

Geo-social Networking is a kind of interpersonal interaction in which geographic administrations and capacities, for example, geo-coding and geo-tagging are utilized to empower extra social flow. Client submitted area information or geo-location systems can permit informal organizations to associate and direction clients with neighborhood individuals or occasions that match their hobbies. Geo-location on electronic interpersonal organization administrations can be IP-based. For versatile informal organizations, messaged area data or cellular telephone following can empower area based administrations to enhance interpersonal interaction. These permits clients to interface with respect to their current areas. Web mapping administrations with geo coding information for spots (roads, structures, and parks) can be utilized with geo labeled data (meet ups, show occasions, dance club or eatery audits) to match clients with a spot, occasion or nearby gathering to associate in or empower a gathering of clients to choose a meeting movement. Famous geo-social applications like Yelp, Gowalla, Face book spots and Foursquare permit clients to impart their areas and also suggestions for an areas or 'venues'.

Location privacy is very important to the maximum number of people who are intended not to reveal their location identity. Through many security issues the location of the particular person is not to be revealed. Location based application services provide location privacy concerns that is used to provide privacy to the location of the user. Location sharing became a common task between people in social communities. Hence the issue here is not to share the location of the user publicly but between the friends of social groups to whom the user intended to share.

Now-a-days, Geo-social applications became a part of human lives. As these systems are misused by someone to extract users personal data, LocX provides improved privacy and with quite certain results. Here the coordinate transformations are used only by friends of particular user. Without accessing the private data of the user, this allows the server to work properly. The coordinate transformations preserve distance metrics, enhancing the task of server to perform queries on transformed data. In this mechanism three types of queries are used and they are circular queries, point queries, neighbor queries. But when the messages are stored in the database it becomes burden to the server to store large number of files and also requires more time.

Hence, the proposed system introduces provider server with the use of LZW compression algorithm which is fast and also simple to apply. As this is a lossless compression technique, the data in the files do not get lost during or after the compression. Sender initially sends the GPS location as in the case of LocX mechanism uses transform coordinates and save it to the index server. In the provider server the details of the users and the data which is stored can be managed. With the compression technique the file is compressed and then the encryption is applied. By this compression technique large files are used to send to the mobile devices having less memory than the normal computers. Key hash tags and random tags are also used to improve the privacy and performance of the system.

Literature Survey

Bugra Gedik and Ling Liu [5] proposed k-anonymity model to protect the location privacy from different privacy threats in location data sharing. This approach involves mainly two features. The main highlight gives bound together protection personalization structure to bolster area k-anonymity for numerous numbers of clients. This methodology empowered every versatile hub by indicating the base level of namelessness and greatest fleeting and spatial resolutions. The second highlight is message bother motor which runs by the area insurance specialist on a trusted server furthermore performed area anonymization on versatile client location based services (LBS) appeal messages.

P.Kalnis, G.Ghinita, K.Mouralidis and D.Papadias [7] developed some methods to protect the privacy of users that is making an issue over spatial queries against location based attacks. Specifically prevents the attacker from inferring the identity of query source over adopting k-anonymity technique to the spatial domain. The user uses a anonymizer when required some data using location based services without disclosing it. He establishes the secure connection with anonymizer and he will delete the identification of the user and transforms his location through cloaking. Cloaking is the technique which hides the exact location of the user by the k-anonymity spatial region(K-ASR or ASR), which is an area that enclosed the client. The anonymizer than sends the ASR to the LBS, which returns a set of candidate results to the anonymizer.

G.Ghinita, P.Kalnis and S.Skiadopoulos [2] introduced PRIVE, a distributed system for query anonyimization in location based services. It supports HILBASR anonyimization technique that makes sure among any user distribution. Experimentally it is shown that PRIVE is a system that is efficient, scalable, fault tolerant and achieved load balancing. In PRIVE, K-ASRs are built in a decentralized fashion and hence bottleneck of centralized server is avoided. This approach hurts the accuracy and also the timeliness of the responses from the server.

Dario Freni, CarmenRuizVicente, SergioMascetti, ClaudioBettini and Christian S.Jensen observed two privacy challenges that affect Geo-social networks. They are location privacy and absence privacy. Location privacy deals with the data of presence of a client at a given location at a particular time. Whereas the absence privacy deals with the data absence of the client at a given location at a particular time. So that lot of sensitive data regarding presence or absence of a user at a location exposed to privacy vulnerability threats which leads to stalking.

Stavros Papadopoulos, Dimitris Papadias and Spiridon Bakiras focused on k-nearest neighbor (KNN) queries and defined the thought of solid area protection which renders the question vague from any area in the information space. It initially introduces Private Information Retrieval (PIR) technique for strong location privacy. This is an efficient technique but the drawback is it is very expensive. And then it presented a novel scheme called AHG to handle them.

Problem Definition

Because of the tremendous growth in mobile technology, various geo-social applications are developed. These geo-social applications are used to find the locations of the user and to share the information of the user. As the location data is shared publicly, that creates threats to the users sensitive data. The location data can be used for malicious purposes. Due to these threats the location of the user is to be hidden from the outer world. By separating the location information and the location data, location privacy can be achieved. In the existing system, the query performance depends on varying put message sizes of the system and stores them on different servers. As the location puts of each user increases, then the size of data will totally increases and hence large data wants to be processed and query answers size increases. The recommendations from the users can be saved and accessed efficiently irrespective of message size.

Proposed System

Actually in this system, the user who is intended to share the location to his friends initially gets his coordinate transformations (x,y) from the GPS system. These coordinate transformations are sent to the friends with rotation angle and shift as (x',y'). These coordinates are transformed to the friends along with some encrypted secret message. The message is sent through some secured media such as email. The transformed coordinates along with the encrypted index will be saved on to the index server. The corresponding location data is encrypted with the secret message.

The data is compressed by using compression algorithm in the provider server module for the efficient retrieving of the data from the data server. The multiple reviews are presented for the same location from the user social group and also from the unknown users. The hash code is used which helps to distinguish these two groups .Hence the index server containing more than exact fields for the hash code that can be used by the user's friend for query will be. To improve the efficiency and the performance of the system, it adds another module i.e., provider server module in which the data of the entire system can be managed. It is done by using the compression mechanism that compresses the data and then stores it in the data server.

When the friend of the user intended to access the reviews of particular location he then again transforms the coordinates and sends the query to the index server. He then retrieves the index by the use of secret key. When the index has been retrieved, a separate query will be obtained on to the data server to get the review. This obtained review first will be decompressed and then decrypts with the same secret key. By this way the location data of the user is secured within the circles of user social groups without getting exposed to the outer world.

The flow of the process that takes place in the system is shown in the following diagram. The way in which the system operations taken place are discussed in the particular diagram.

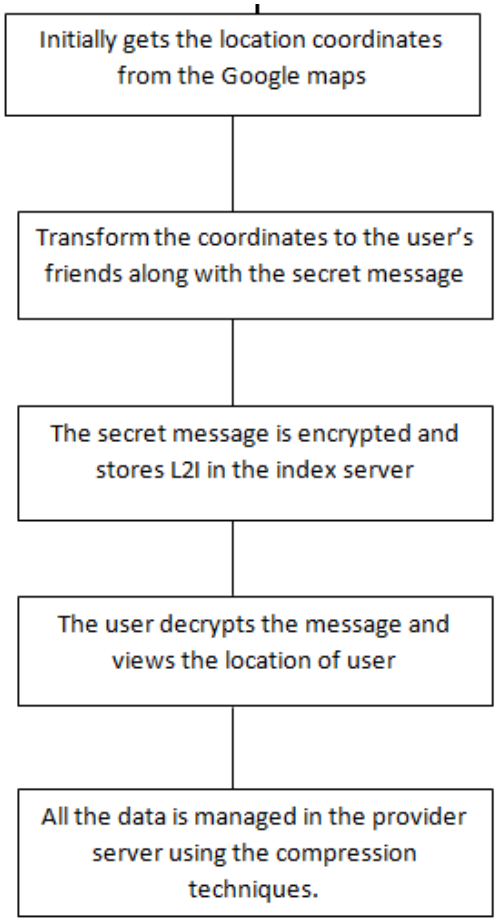


Figure 1: Overview of system operations

The proposed system uses following four algorithms to provide privacy to the Geo-social applications**.**

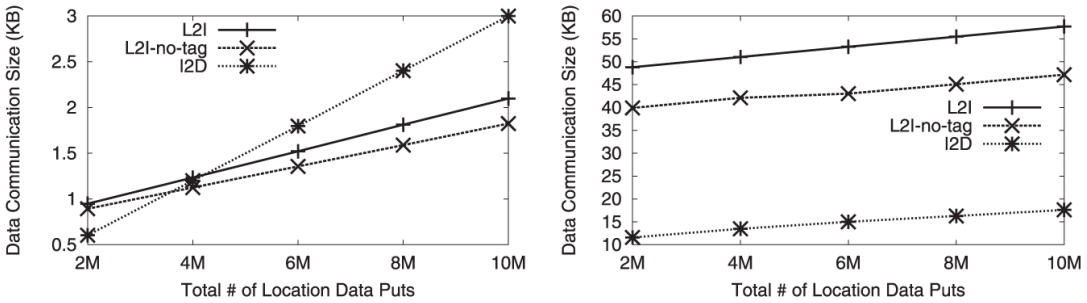
1. Compression algorithm:
The entire data of the user is stored in the database that becomes larger sized files. These files are compressed using the data compression algorithm to reduce the burden of the server. The user gets the compressed files from the database.

2. Decompression algorithm:
The user gets the compressed data files from the database. By using the decompression algorithm, the compressed files will be decompressed.

3. AES encryption algorithm:
AES encryption algorithm provides high security and hence it is used to encrypt the location transformations in the system. This location data is encrypted before it will send to the server for storage purpose. Hence the data will be secured even though the attacker gets this information.

4. AES decryption algorithm:
This AES decryption algorithm is used to decrypt the location information as the actual information is necessary for processing the system.

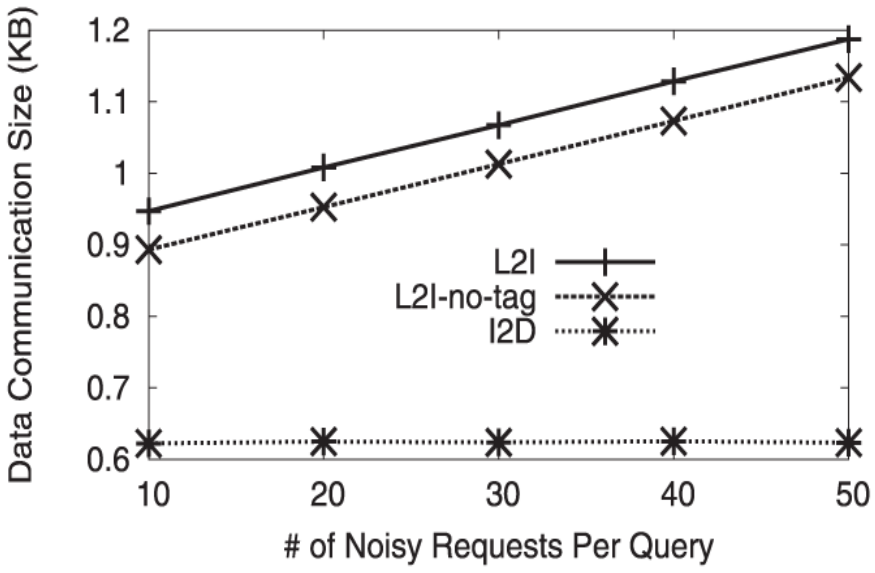
5. Results:
The breaking down of communication overhead from L2Is and the I2Ds when the number of puts is increased is plotted in the following graph.



(a) Point Queries (b) Nearest Neighbor Queries

The overhead from L2I and I2D is done separately. This overhead from L2I in the setting where no labels are connected is alluded to as 'L2I-no-tag'. It is shown in Figure (a) that as the quantity of puts increments, more information is returned as answers and the correspondence expense of I2D increments more than that of L2I for point inquiries. Anyhow, on account of closest neighbor questions, since a considerable measure of information needs to be sifted in L2I stage, more information is transmitted for L2Is. Conversely, just qualified answers are transmitted in I2D stage. As shown in figure b, the communication cost of L2I is more than that of I2D.

The increase in the L2I communication overhead due to the increase in noise is plotted in the following graph for point queries in synthetic data.



The amount of noise added per query is varied from 10 to 50, while fixing the other parameters to default. Above figure shows that increase in the noise only increases the communication overhead from L2I, and thus this particular increase is quite small. No increase in I2D overhead is not be there due to noise. Also the noise will not raise the computation time on users devices, as users will not accept responses to noisy points and not even attempt to decrypt them. The usage for kNN queries is same, but the graph is left out as there is no space.

Conclusion

This paper discussed about the security, location privacy and the increase in performance of location based social network system. A protocol is designed that provides the security and privacy that recognizes completeness and correctness. A provider server module is used to manage all the data of the user and the data is compressed using compression techniques.

The existing system for Geo-social applications takes time to transmit the data to the server. The more time is taken when the message size is large that degrades the system performance. The proposed system overcomes the drawback of LocX system and also improves the performance of the system using a new module with the compression techniques.

References

[1] M.Gruteser and D.Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking, Proc. First Intl Conf. Mobile Systems, Applications Services, 2003

[2] G. Ghinita, P. Kalnis, and S. Skiadopoulos, PRIVE: Anonymous Location Based Queries in Distributed

[3] 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.

[4] M. Motani, V. Srinivasan, and P.S. Nuggehalli, PeopleNet: Engineering a WirelessVirtual Social Network, Proc. ACM MobiCom, 2005

[5] B. Gedik and L. Liu, Location Privacy in Mobile Systems:A Personalized Anonymization Model, Proc. IEEE 25th Intl Conf.Distributed Computing Systems,2005.

[6] T.Jiang, H.J. Wang, and Y.-C. Hu, Preserving Location Privacy in Wireless Lans, Proc. Fifth Intl Conf. Mobile Systems, Applications Services, 2007.

[7] 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.

[8] B. Schilit, J. Hong, and M. Gruteser, Wireless Location Privacy Protection, Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.