Preserving Location Privacy In geosocial Application

Chavan Pratibha, Bandal Shital, Chaudhari Shubhangi, Bhujbal Sumit

Computer Dept. Jaywantrao sawant collage of Engg. , Pune

Abstract:

Recently privacy is important issue in our daily life. We must have to take care of our data. But this is not possible every time, sometimes because of busy schedule we can't take care of our data. So, we proposed to build an application of mobile, preserving location privacy System using cloud. Our system provide a location information. Our application provide easy way to secure our location data. Silent features of our preserving location privacy system are to provide security to location, provide primary solution to preserve particular location data, and provide friends locations. We also provide privacy. This system or application is most useful in emergency cases. With the help of this system friends can check location of the user and according to he can meet with that particular user. Friends or user can also check for nearby friends.

Keywords: K-NN, LocX, LBSA,

Introduction:

We efficiently protect user privacy in the system, or making good assumptions about the security or trustworthiness of the application servers. Mainly we target geosocial applications, and assume that servers can be compromised to limit misuse.

1) Our goal is to limit accessibility of location information from global visibility to a user’s social circle. We identify two main types of queries needed to support the functionality of these geosocial applications.

2) Point queries and nearest-neighbor (kNN) queries. Point queries query for location data at a particular point, whereas kNN queries query for k nearest data around a given location coordinate. Our goal is to support both query types in a suitable for today’s mobile devices.

3) We propose Loc X, a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications. Our insight is that many services do not need to
resolve distance-based queries between arbitrary pairs of users, but with only those friends which are interested in each other’s locations and data.

4) We can partition location data based on social groups, after performing transformations on the location coordinates before storing them on any servers. A user knows the transformation keys of all his friends, allowing her to relocate query into the virtual coordinate system that her friends use. Our coordinate transformations is used to preserve distance metrics, with permission to an application server to perform both points and nearest-neighbor queries correctly on transformed data.

5) The applications implemented on Loc X lightweight and suitable for running on today’s mobile devices by using 2d-Translation, 2d-Scaling & 2d-Rotation algorithm.

Related Work:

Parsons have proposed accountability mechanisms to address privacy concerns of end users and then develop a privacy manager. The idea is that the user’s private data are sent to the cloud there that will converted in an encryption form of data, and the processing is done on the encrypted data. The output of the process is data which is in decrypted format by the privacy manager to reveal the correct result if that particular other user or friend enters that key. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed.

Literature survey:

<table>
<thead>
<tr>
<th>Sr. NO.</th>
<th>YEAR</th>
<th>PAPER NAME</th>
<th>AUTHOR</th>
<th>CONCEPT/ALGORITHM USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>Event Details</td>
<td>Paper Title</td>
<td>Authors</td>
<td>Key Points</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>2010</td>
<td>3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)</td>
<td>“Privacy preserving based on association rule of mining”</td>
<td>Tinghuai Ma, Sainan Wang, Zhong Liu</td>
<td>Data mining technology is used and try to resolve privacy problem, Data hiding.</td>
</tr>
<tr>
<td>2014</td>
<td>IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014</td>
<td>“Preserving location privacy in geosocial applications.”</td>
<td>Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal</td>
<td>In this collaboration of cloud computing, data mining &amp; android security by using LOCx technique and 4-square technology</td>
</tr>
</tbody>
</table>
Architecture:

Fig.1 Architecture of systems

Future Work:

The project ensuring distributed data sharing and security in android & cloud is to. After uploading data on cloud this project will maintain all the records about user who have used the data. Also bundling of the file with its information and accessing that data or location by getting that particular key & through that we can preserve our location is the scope of the system.

Conclusion:

This paper explains the design, prototype implementation, and evaluation of Loc X, a system for building location-based social applications (LBSAs) while preserving user location privacy. Loc X provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components. Loc X takes a novel approach to provide location privacy while maintaining overall system efficiency, by leveraging the social data-sharing property of the target applications. In Loc X, users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties. Using evaluation based on both synthetic and real-world LBSA traces, we find that Loc X adds little computational and communication overhead to existing systems. Our Loc X prototype runs efficiently even on resource constrained mobile phones. Overall, we believe that Loc X takes a big step toward making location privacy practical for a large class of emerging geosocial applications.
Acknowledgment:

The authors would like to thank the researchers and publishers for making their resources available and teachers for guidance. We also thank to the college authority for supporting to us and providing required information. We would also like to thank our friends and family members.

References:

[1] Smitha Sundarwaran, Anna C. Squicciarini, member, IEEE, and Dan Lin “Ensuring Distributed Accountability For Data Sharing in the Cloud” IEEE transactions on dependable and secure computing vol.9 no.4, year IEEE 2012..


