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 5, May 2015

To Enhance Recommendation By Providing Location Privacy In GeoSocial Application

Charushila Kapde[1], Priyanka Kumbhar[2] , Reena Gandhi[3], Bindu Pandit[4], S. S. Sambare[5]

UG Student, Dept. of Computer, PCCOE, Pune , Savitribai Phule University, Maharashtra, India[1,2,3,4]

Professor, Dept. of Computer, PCCOE, Pune , Savitribai Phule University, Maharashtra, India[5]

ABSTRACT: Now a days there are many geo social applications which are based on large extent, so people are more concern about the security of location and respective data stored at that location. But the location privacy provided is not enough. In this paper, we are using LocX, which is a new approach for improving location privacy without adding ambiguity or relying on strong assumptions. User stores encrypted data on the server by using transformations. When user allows recommender then they can access the users location and data. LocX provides more privacy for today's mobile devices.

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

I. INTRODUCTION

Geo social networking is a type of social networking in which geographic services and capabilities such as geo coding (location) and geo tagging (metadata) are used to enable additional social dynamics. For mobile social networks , texted location information or mobile phone tracking can enable location based services to enrich social networking .User submitted location data or geo location techniques, these kind of information can allow social networks to connect and coordinate users with other people or events having same interest area.

It is a recognized fact that the evolution of personal communication devices leads to serious concerns about the location privacy issues. In response to these issues, during last decade many Location-Privacy Protection Mechanisms (LPPMs) have been proposed. The assessment and comparison remains problematic because of the absence of a systematic method to quantify the issues. Many services do not need to determine distance-based queries among random pairs of users, but only between the friends interested in each others data and locations. Thus, partition can be done on location data based on users social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user should know the transformation keys of all users friends, allowing to transform query into the virtual coordinate system that users friends uses. Transformations of coordinates preserve distance metrics, 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- 1 world locations without a secret, which is only available to the members of the social group. Finally, 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. Now a days, the geosocial applications have come very close to a common man. Now these applications are being used for different purposes such as social recommendations. It is very likely that in the future these applications will be the primary source of information. But with the growth of technology, the risk of privacy regarding personal information has also increased. And these applications are useless without ensuring privacy to its user as studies have indicated that users will express very strong concern about privacy to their personal information. So, we need to adopt a design process for reliable access of these applications as per the present need and demand of the user.[3] Without sufficient location protection, however, these systems can be easily misused, In this paper, we introduce, a technique that provides location secrecy without adding complexity into query results.

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 5, May 2015

II. RELATED WORK

ICliqueCloak

Privacy protection has recently received considerable attention in location based services. A large number of location clocking algorithms have been proposed for protecting the location privacy of mobile users. By considering the scenario where different location-based query requests are continuously issued by mobile users while they are moving. The system shows that most of the existing k-anonymity location cloaking algorithms are concerned with snapshots user locations only and can not effectively prevent location dependent attacks when users' locations are continuously updated. Therefore, adopting both the location k-anonymity and cloaking granularity as privacy metrics, a new incremental clique-based cloaking algorithm, called ICliqueCloak,is used to defend against location-dependent attacks. [2]The main idea is to incrementally maintain maximal cliques needed for location cloaking in an undirected graph that takes into consideration the effect of continuous location updates. Thus, a qualified clique can be quickly recognized and used to generate the cloaked region when a new request comes. The efficiency and effectiveness of the proposed ICliqueCloak algorithm are validated by a series of carefully designed experiments.The experimental results also show that the price paid for defending against location dependent attacks is small. The second category is location transformation, which uses transformed location coordinates to preserve user location privacy. One subtle issue in processing nearest neighbor queries with this approach is to accurately find all the real neighbors. Blind evaluation using Hilbert Curves, unfortunately, can only find approximate neighbors. To find real neighbors, previous work either keeps the proximity of transformed locations to actual locations and incrementally processes nearest-neighbor queries, or requires trusted third parties to perform location transformation between clients and LBSA servers.

Casper

Casper a framework in which users entertain anonymous location-based services. Casper consists of two main components; the location anonymizer that blurs the users' exact location into cloaked spatial regions and the privacy-aware query processor that is responsible on providing location-based services based on the cloaked spatial regions. While the location anonymizer is implemented as a stand-alone application, the privacy-aware query processor is embedded into PLACE (a research prototype for location-based database servers).[6]

Foursquare

Foursquare is a local search and discovery service mobile app which provides a personalized local search experience for its users. By taking into account the places a user goes, the things they have told the app that they like, and the other users whose advice they trust, foursquare aims to provide highly personalized recommendations of the best places to go around a user's current location. Foursquare is a location-based social network to check in to users favorite locations and let users friends know users location. Foursquare have deeper purposes than just location sharing with friends, though. Many restaurants and stores will reward loyalty and frequent check-ins with specials and deals. In order to use Foursquare, user must have a GPS or Internet enabled phone. Once user is in a location - for example, Bobst Library - you can check in to Foursquare and let users friends know users location. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. It is a risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices, and even on the servers in answering queries such as nearest neighbor and range queries.[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 5, May 2015

III. PROPOSED ALGORITHM

A. Implementation and setup

We implemented LocX application using Java (J2ME toolkit). We used AES algorithm with 128 bits keys for the encryption and decryption of data and index. The implementation of nearest-neighbor queries was based on the R--tree package from HKUST. We measured performance of LocX on two desktops. The index and data servers were run on the same desktop with
Processor: Any Processor above 500 MHz.
Ram: 1 GB.
Hard Disk : 10 GB.
Compact Disk: 650 Mb.
Input device: Standard Keyboard and Mouse.
Operating System: Windows 7
Technology: Net Beans 8.0 Jdk7.
Clients were run on another machine with the same configuration. We used the same code base for both desktop and mobile tests.

Workload.
We used synthetic and real-world LBSA workload datasets for our tests. Here, we used j2me toolkit instead of desktop users.A midlet is an application that uses the Mobile Information Device Profile (MIDP) of the Connected Limited Device Configuration (CLDC) for the Java ME environment.

B. Performance Requirements

When an application is developed to run on a particular software platform such as J2ME, Android, etc, it can in theory be installed and run on any device that supports that platform. However for any given platform, the supported devices could have a very wide range of capabilities in terms of CPU speed and available memory. For example a J2ME application can be theoretically run on a low end feature phone such as the Nokia 3230 with a 123 MHz CPU and 6 MB of RAM as well as the high end Nokia N8 with 600+MHz CPU and 256 MB RAM. However it has been designed to require a certain minimum CPU power and memory, it might in practice, fail on the Nokia 3230 phone. If an application makes extensive use of arithmetic and logic operations such as those involved in streaming and decompression of audio and video and in rich animations, or it lets the user view and manipulate large sets of information or images, you should specify minimum CPU and memory requirements for the application in exactly the same way it is done for desktop applications.

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 5, May 2015

Locx system

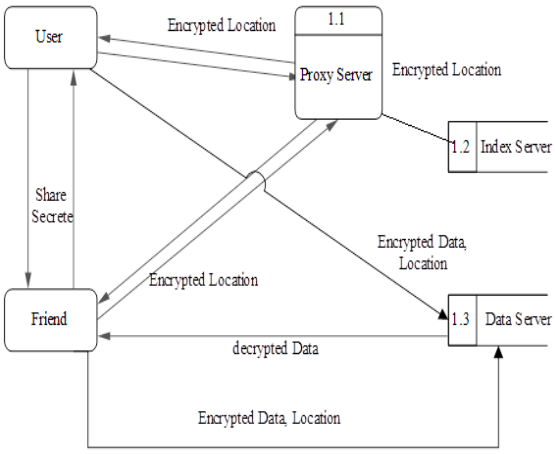

Fig. System architecture

In this design consider an example,

1) Friends can exchange their secrets among themselves.
2) User stores his review of the restaurant (at(x,y)) on the server under transformed coordinates.
3) Later when friend visits the restaurant and queries for the reviews on transformed coordinates
4) After decryption 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 three types of servers – index, data, proxy 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 conserves 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.

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 5, May 2015

Storing I2Ds on the data server

The user can directly store I2Ds (location data) on the data server. 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 while querying. The queries only contain a list of points in the transformed coordinate space.

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.

IV. PSEUDO CODE

1. Create a network having three servers such as proxy server, LBSA server and Location server with a user interface (MIDP Application).

2. User should register themselves in the network then user id and password will be assigned to each user.

3. If user want to store his/her data on particular location where he/she visited then on a transformed coordinates (x', y') he will store the data in encrypted format.

4. With the help of pseudorandom key generator, user is going to generate secret key and with this secret key user's friend can access users data. This key is shared between the friends.

5. If user's friend want to access users data then friend has to find out secret key .

```
if(users key = friends key) then
{
    if(user allow = true)then
        {
            Friend will get to know the location index in encrypted format then friend will
        decrypt it.
            if(decrypted_ index=users_index)then
                {
                    Friend will get the encrypted data
                }
                Else
                Retry()
        }
        Else
        {
            Data access denied
```

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 5, May 2015

```
                }
}
Else
{
        Ask for correct secret key.
}
6.End
```

V. SIMULATION RESULTS

As n number of users are using application they need their respective secret key. The particular secret key is generated by using random key generator algorithm. User should first register themselves in the network for accessing LocX application. We are providing various functions to make the system user friendly like:

1) Finding location

We can see the location on google maps and with the help of transformed coordinates we can store the data on that particular location.

2)Location update

User can update their respective location and all other remaining users will be notified about it. Providing all privacy aspects user can retrieve the data by using the decrypted index.

3)Location Recommendations

Users can give their recommendations which will get stored at respective location. All other users can see recommendations if they are authorized.

VI. CONCLUSION AND FUTURE WORK

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 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.

REFERENCES

1. Ahmad F,Abdul Matin,"A novel positioning technique for Context Awareness",IEEE 2014.
2. Xiang Fu,Chongjain Liu,"Extended clique models:A new matching strategy for fingerprint recognition",Biometrics Compendium,IEEE 2013.
3. Krishna P. N. Puttaswamy, Shiyuan Wang, \Preserving Location Privacy in Geo- Social Applications", Department of Computer Science, UC Santa Barbara IEEE 2012.
4. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, Location Privacy via Private Proximity Testing, Proc. Network Distributed System Security Conf., 2011.
5. 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.
6. M.F. Mokbel, C.-Y. Chow, and W.G. Aref, The New Casper: A Privacy-Aware Location-Based Database Server, Proc. IEEE 23rd Intl Conf. Data Eng., 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.