International Journal of Emerging Technologies in Engineering Research (IJETER)
Volume 5, Issue 6, June (2017) www.ijeter.everscience.org

Preserving Location Based Range Query over Outsourced Data with EPLQ Using LOCX

M. Karthika
P.G. Scholar, MIET Engineering College, Trichy, Tamilnadu, India.

Dr. K. Geetha
Associate Professor, Dept. of Computer Science and Engineering, MIET Engineering College, Trichy, Tamilnadu, India.

Dr. D.Yuvaraj
Professor and Head, Dept. of Computer Science and Engineering, MIET Engineering College, Trichy, Tamilnadu, India.

Abstract – Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. However, the use of LBS also poses a potential threat to user's location privacy. In this paper, LocX, a novel alternative is introduced which provides significantly-improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access.

Index Terms – Location-Based Services, *LocX*, Attribute Based Encryption, K Nearest Neighbor.

1. INTRODUCTION

With billions in downloads and annual revenue, smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. The explosive popularity of mobile social networks such as SCVNGR and FourSquare likely indicate that in the future, social recommendations will be our primary source of information about our surroundings. For current services with minimal privacy mechanisms, this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain, physical stalking, and to gather legal evidence.

1.1 PRIOR WORK ON PRIVACY IN GENERAL LOCATION-BASED SERVICES

There are mainly three categories of proposals on providing location privacy in general LBSs that do not specifically target social applications. First is spatial and temporal cloaking wherein approximate location and time is sent to the server instead of the exact values. This approach, however, hurts the accuracy and timeliness of the responses from the server, and most importantly, there are several simple attacks on these mechanisms that can still break user privacy.

Pseudonyms and silent times are other mechanisms to achieve cloaking, where in device identifiers are changed frequently, and data is not transmitted for long periods at regular intervals. This, however, severely hurts functionality and disconnects users. In LocX, we do not trust any intermediaries or servers. On the positive side, these approaches are more general and, hence, can apply to many location-based services, while LocX focuses mainly on the emerging geo-social applications.

1.2 DECOUPLING A LOCATION FROM ITS DATA

In today's systems, location data data(x,y) corresponding to the real-world location (x, y) is stored on the server. But in LocX, the location is first transformed to the server and the location data is encrypted . Then the transformed location is decoupled from the encrypted data using a random index i via two servers as follows: which stores E(i) under the location coordinate , and 2) an I2D, which stores the encrypted location data under the random index i.

1.3 TERMINOLOGY

Location coordinates refer to the longitude, latitude pairs associated with real-world locations. A pair of coordinates is returned from a GPS, and is used to associate data with a location. Location data or location information refers to such data associated with a location.

1.4 SYSTEM AND ATTACKER MODEL

In this paper, we assume that the companies that provide LBSA services manage the servers. Users store their data on the servers to obtain the service.The companies are responsible for reliably storing this data,and providing access to all the data a user should have access to. The companies can get incentives via displaying ads, or charging users some usage fees. In our attacker model, we assume that the attacker has access to the LBSA servers.

The attacker might even be an oppressive regime or a government that obtains data from the providers via subpoenas. As a result, in our model, the attacker can access all the data stored on the servers, and can also monitor which user device is accessing which pieces of information on the servers.

2. EXISTING SYSTEM

In the existing system a novel predicate-only encryption scheme for inner product range named IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. In particular, a POI matches a spatial range query or not can be tested by examining whether the inner product of two vectors is in a given range.

2.1 Demerits of Existing System

- Querying encrypted LBS data without privacy breach is a big challenge
- High computational cost and/or storage cost at user side.
- The techniques used to realize privacy-preserving query usually increase the search latency.

2.2 PROPOSED SYSTEM

In the proposed system *LocX*(short for location to index mapping), 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 only between friends interested in each other's locations and data. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data.

2.3 Merits of Proposed System.

- Our techniques have potential usages in other kinds of privacy preserving queries
- Cost will be less compared to existing system.

3. SYSTEM DESIGN

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

System Design For Admin

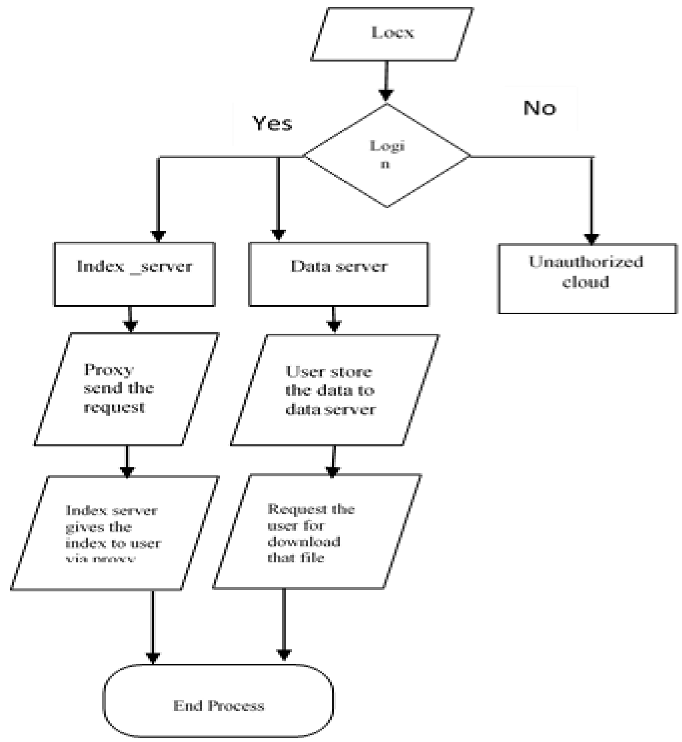


Fig 3.1 : System Design for Admin

User

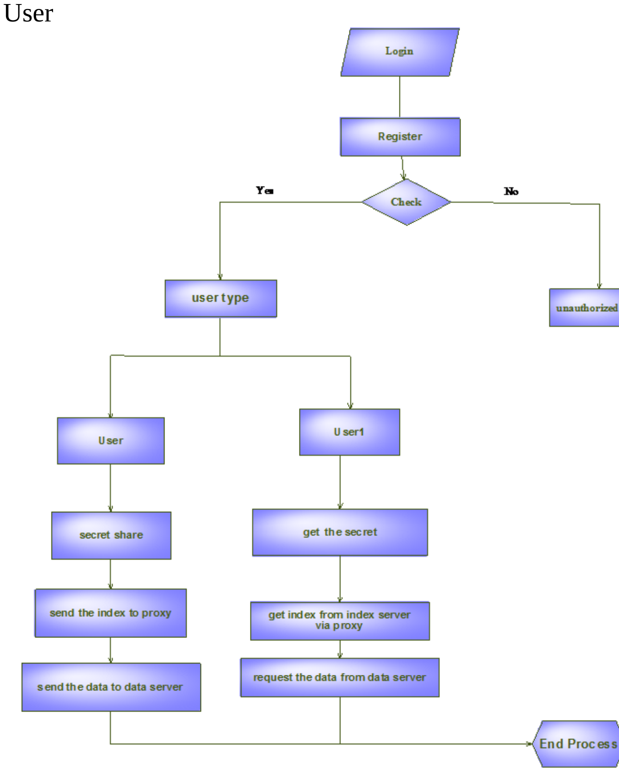


Fig 3.2 : User Diagram

Activity Diagram

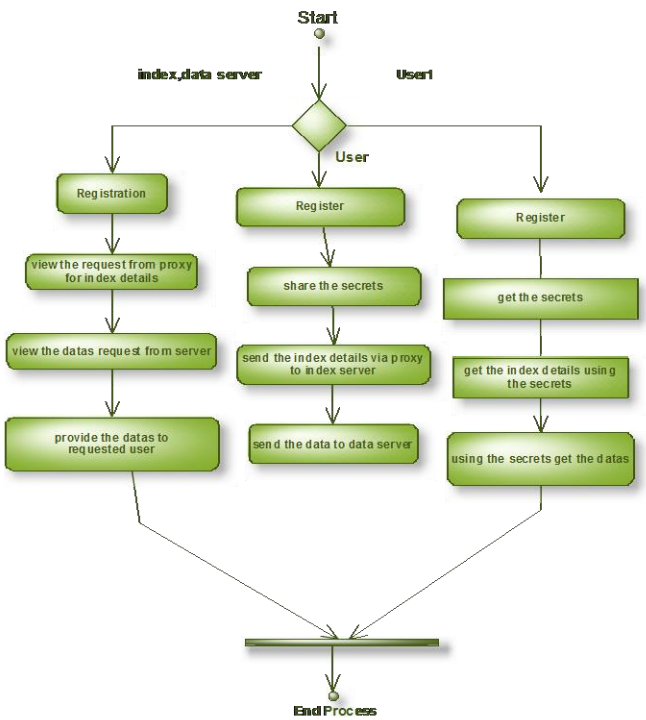


Fig 3.3 : Activity Diagram

SEQUENCE DIAGRAM

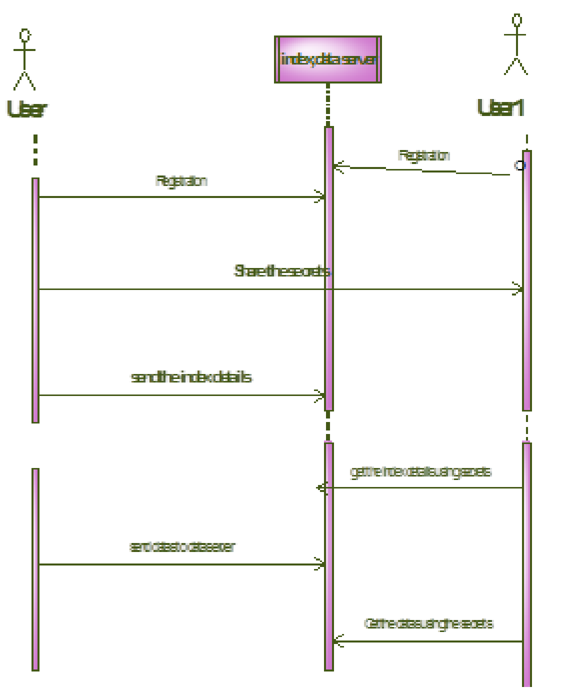


Fig : 3.4 : Sequence Diagram

4. MODULE DESCRIPTION

4.1 LOCX:

LocX builds on top of the basic design, and introduces two new mechanisms to overcome its limitations. First, in LocX, the mapping between the location and its data split into two pairs: a mapping from the transformed location to an encrypted index and a mapping from the index to the encrypted location data. This splitting helps in making our system efficient. Second, users store and retrieve the L2Is via un trusted proxies. This redirection of data via proxies, together with splitting, significantly improves privacy in LocX.

4.2 Proxying Location to an Encrypted Index

Users store their location to index on the index server via untrusted proxies. These proxies can be any of the following: PlanetLab nodes, corporate NATs and email servers in a user's work places, a user's home and office desktops or laptops, or Tor nodes.. These diverse types of proxies provide tremendous flexibility in proxying location to index, thus a user can store there location to index via different proxies without restricting herself to a single proxy. Furthermore, compromising these proxies by an attacker does not break users' location privacy, as (a) the proxies also only see transformed location coordinates and hence do not learn the users' real locations, and (b) due to the noise added toL2Is

4.3 Storing L2I on the index server

First consider storing L2I on the index server. This transformation preserves the distances between points1, so 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. Then the user generates a random index (i) using the random number generator and encrypts it with the symmetric key to obtain at the transformed coordinate on the index server via a proxy. The L2I is small in size and is application independent, as it always contains the coordinates and an encrypted random index. Thus the overhead due to proxying is very small.

4.4 Storing I2DS on the Data server.

The user can directly storeI2Ds (location data) on the data server. This is both secure and efficient.

1) This is secure because the data server only sees the index stored by the user and the corresponding encrypted blob of data. In the worst case, the data server can link all the different indices to the same user device, and then link these indices to the retrieving user's device .But this only reveals that one user is interested in another user's data, but not any information about the location of the users, or the content of the I2Ds, or the real-world sites to which the data in the encrypted blob corresponds to.

2) The content of I2Dis application dependent. For example, a location-based video or photo sharing service might share multiple MBs of data at each location. Since this data is not proxied, LocX still maintains the efficiency of today's systems.

5. IMPLEMENTATION

The user knows the transformation keys of all their friends, allow to transform the query into the virtual coordinate system that their friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data.

The user sends the co-ordiates to the requested user The msg which was send by the user is forward to the LOCX server.The users send the location by using smart phone. The encrypted information will be forward to LOCX

Users store their location to index on the index server via untrusted proxies.

LocX, the mapping between the location and its data split into two pairs: a mapping from the transformed location to an encrypted index and a mapping from the index to the encrypted location data.

The user generates a random index (i) using the random number generator and encrypts it with the symmetric key to obtain at the transformed coordinate on the index server via a proxy

6. PROGRAM

6.1 Application Program Snippet

```
package com.example.cbac;
import android.os.Bundle;
import android.app.Activity;
import android.view.Menu;
public class AboutApp extends Activity
{
    @Override
protected void onCreate(Bundle savedInstanceState)
{
super.onCreate(savedInstanceState);
setContentView(R.layout.activity_about_app);
}
@Override
public boolean onCreateOptionsMenu(Menu menu)
{
getMenuInflater().inflate(R.menu.about_app, menu);
return true;
}
}
```

6.2 Main Activity Program Snippet

```
import android.os.Bundle;
import android.os.Handler;
import android.app.Activity;
import android.content.Intent;
import android.content.SharedPreferences;
public class MainActivity extends Activity
{
SharedPreferences sp;
Intent i;
@Override
protected void onCreate(Bundle savedInstanceState)
{
setContentView(R.layout.activity_main);
sp=getSharedPreferences("register", MODE_PRIVATE);
    Handler h=new Handler();
    h.postDelayed(new Runnable()
{
                @Override
public void run() {
    // TODO Auto-generated method stub
if(sp.getString("name", "null").equals("null") && sp.getString("pswd", "null").equals("null"))
{
 i=new Intent(MainActivity.this, Registration.class);
    startActivity(i);
    finish();
    }else
    {
     i=new Intent(MainActivity.this, Login.class);
    startActivity(i);
    finish();
```

```
}
}
}, 3000);
}
```

6.3 Activity login XML Program Snippet

```
<LinearLayout
xmlns:android="http://schemas.android.com/apk/res/android"
xmlns:tools="http://schemas.android.com/tools"
android:layout_width="match_parent"
android:layout_height="match_parent"
android:paddingBottom="@dimen/activity_vertical_margin"
android:paddingLeft="@dimen/activity_horizontal_margin"
android:paddingTop="@dimen/activity_vertical_margin"
  tools:context=".Login" >
   <TextView
     android:id="@+id/textView1"
android:textAppearance="?android:attr/textAppearanceLarge"
/>
  <EditText
    android:id="@+id/loginname_editText1"
    android:inputType="textPersonName" >
    <requestFocus />
  </EditText>
  <EditText
    android:id="@+id/loginpswd_editText2"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:inputType="textPassword" />
  <Button
    android:id="@+id/loginbutton1"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
   android:background="@drawable/btn_blue"
    android:text="Sign In" />
  <Button
    android:id="@+id/logincancelbutton2"
    android:layout_width="fill_parent"
    android:onClick="onCancel"
    android:text="Cancel" />
</LinearLayout>
```

7. PROGRAM SCREEN SHOTS

Fig 7.1 : Admin Login

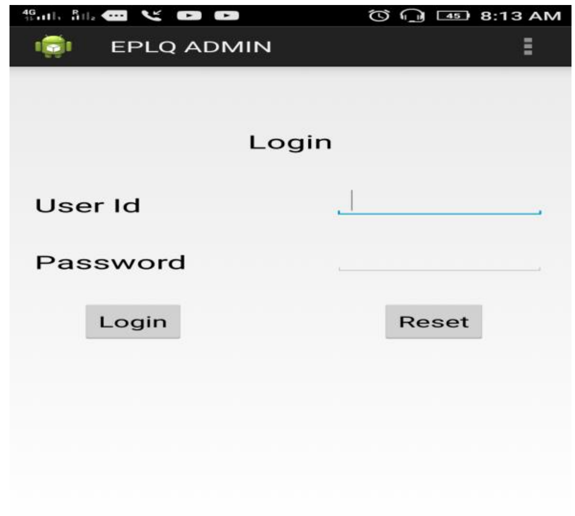


Fig 7.2 : Register for User ID with password

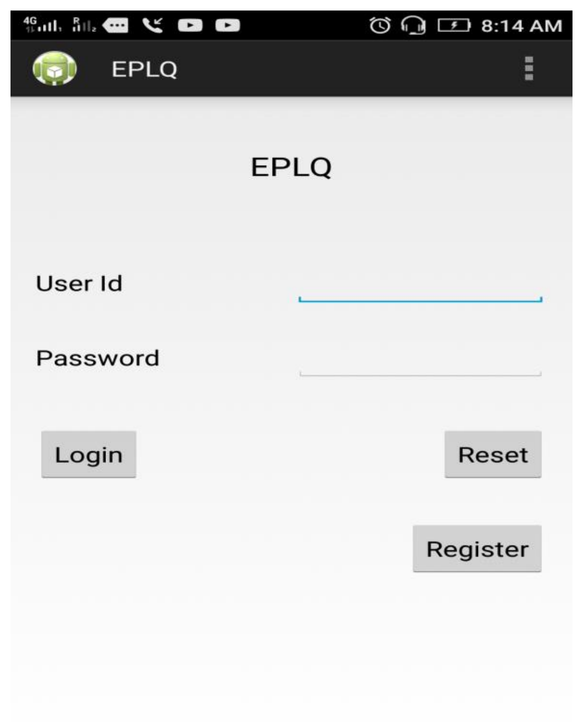


Fig 7.3 : Register Form for New User

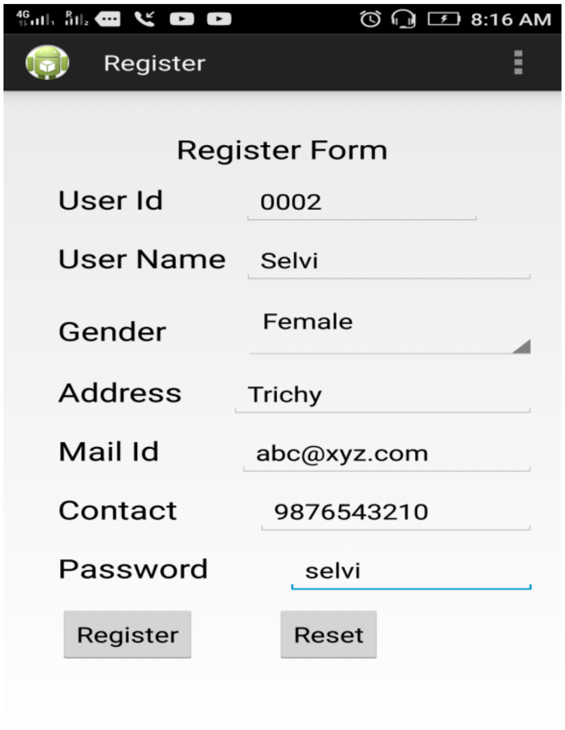


Fig 7.4: Home Screen with Message Status

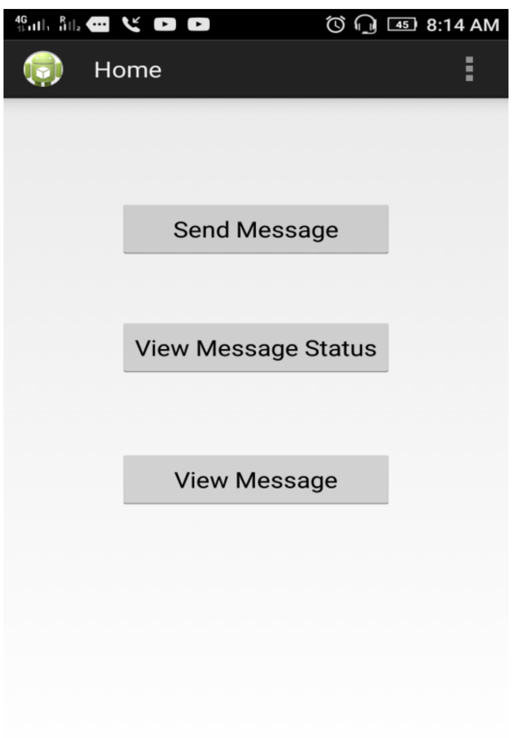


Fig 7.5 : Send Message Details with Lat & Long.

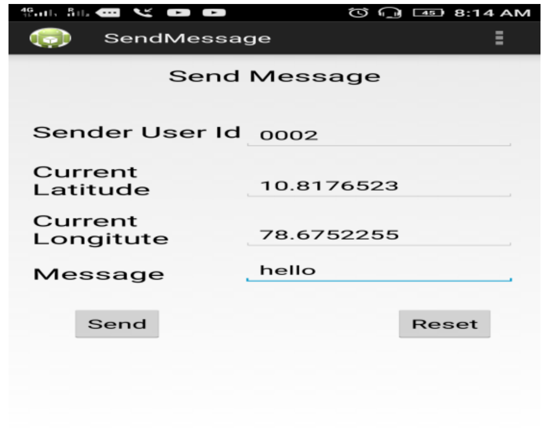


Fig 7.6: EPLQ Window

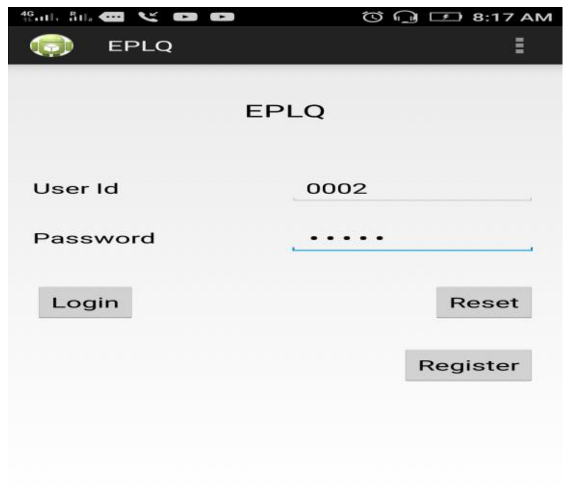
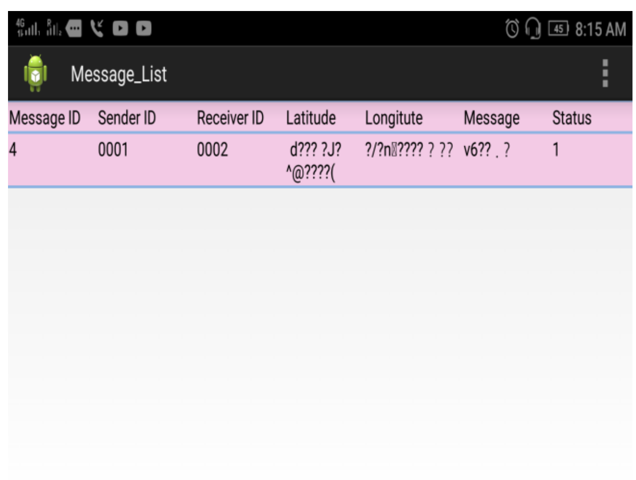


Fig 7.7: Message list.



8. CONCLUSION

LocX provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components. LocX 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 LocX, 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's 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 LocX adds little computational and communication overhead to existing systems.

REFERENCES

[1] A. Gutscher, "Coordinate transformation - a solution for the privacy problem of location based services?" in 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings, 25-29 April 2006, Rhodes Island, Greece, 2006. [Online]. Available: http://dx.doi.org/10.1109/IPDPS.2006.1639681

[2] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in SIGMOD. ACM, 2009, pp. 139–152.

[3] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in SIGMOD. ACM, 2008, pp. 121–132.

[4] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in ICDE. IEEE, 2014, pp. 640–651.

[5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," Journal of the ACM (JACM), vol. 45, no. 6, pp. 965–981, 1998.

[6] F. Olumofin and I. Goldberg, "Revisiting the computational practicality of private information retrieval," in Financial Cryptography and Data Security. Springer, 2012, pp. 158–172.

[7] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings, 2008, pp. 146–162. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-78967-3 9

[8] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, 2007, pp. 535–554.

[9] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[10] D. A. White and R. Jain, "Similarity indexing with the ss-tree," in ICDE . IEEE, 1996, pp. 516–523.

[11] A. Guttman, "R-trees: A dynamic index structure for spatial searching," in SIGMOD'84, Proceedings of Annual Meeting, Boston, Massachusetts, June 18-21, 1984, 1984, pp. 47–57. [Online]. Available: http://doi.acm.org/10.1145/602259.602266

[12] T. K. Dang, J. K¨ung, and R. Wagner, "The sh-tree: A super hybrid index structure for multidimensional data," in Database and Expert Systems Applications, 12th International Conference, DEXA 2001 Munich, Germany, September 3-5, 2001, Proceedings, 2001, pp. 340–349. [Online]. Available: http://dx.doi.org/10.1007/3-540-44759-8 34

[13] B.-Y. Yang and J.-M. Chen, "All in the xl family: Theory and practice," in ICISC. Springer, 2004, pp. 67–86.

[14] G. Ars, J.-C. Faugere, H. Imai, M. Kawazoe, and M. Sugita, "Comparison between xl and gr¨obner basis algorithms," in ASIACRYPT. Springer, 2004, pp. 338–353.

[15] B. Yao, F. Li, and X. Xiao, "Secure nearest neighbor revisited," in ICDE. IEEE, 2013, pp. 733–744.

[16] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments," in ICDE. IEEE, 2014, pp. 664–675.

[17] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in Advances in Spatial and Temporal Databases. Springer, 2007, pp. 239–257.

[18] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidimensional range queries over outsourced data," The VLDB Journal, vol. 21, no. 3, pp. 333–358, 2012.

[19] I.-T. Lien, Y.-H. Lin, J.-R. Shieh, and J.-L. Wu, "a novel privacy preserving location-based service protocol with secret circular shift for k-nn search," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 863–873, 2013.

[20] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," VLDB J., vol. 19, no. 3, pp. 363–384, 2010. [Online].