Securing Location Privacy in Location based Service Applications with Dual Encryption

Anju S
Student
Department of Computer Science and Engineering
Nehru College of Engineering and Research Centre
Pampady, Thrissur, India

Jasmine Joseph
Assistant Professor
Department of Computer Science and Engineering
Nehru College of Engineering and Research Centre
Pampady, Thrissur, India

Abstract

Location Based Service Applications (LBSAs) are becoming a vital part of our lives now. The users can communicate with the physical world and get all information they want through these applications. An example for LBSA is Foursquare .The demerit is it misuses in different ways by exploiting personal data of users and causes many threats. To avoid these threats and to increase location privacy uses the technique LocX. The locations as well as the data added with it are mapped before store in many servers. So the location cannot be retrieved from the server by a third party and the location is not visible to the hackers. Also, to improve the security in location points and data points we introduce dual encryption method in LocX. Asymmetric keys are used to encrypt the data with two keys public key and user's private key. But in LocX random inexpensive symmetric keys are used.
Keywords: Encrypt; Location Privacy; Asymmetric

I. INTRODUCTION

Many services are provided by smart phone applications provided by Android and Apple iTunes. Most commonly used service is GPS location service. It helps to find out the location and data related to it. Foursquare and SCVNGR are one of the most downloaded apps. Anyone can communicate with the physical world and get the details about the locations that their friends shared.

The service's procedure when a user request for services as given below.

1) With the help of positioning device such as GPS, an LBS user obtains the accurate position data of a user
2) The client sends the location data to a service provider.
3) The service provider creates a counter message that reacts to the received position data and sends it back to the client.
4) A reply message is acknowledged by the client.

The common design of Location Based Social Applications (LBSAs) is shown in the Fig. 1. Suppose user A is at restaurant (x, y). He wants to give a review w about the restaurant. He stored the encrypted review E (data) coupled with its corresponding transformed location coordinate (x', y') on the server. Later another user B wants to know what his friend A shared about the restaurant. This is by giving the correct shared key only known by them and will decrypt the data and location. The main limitation of this design is that when A saves the data and location directly to the server, a third party can hack the server and track the users. This will lead to home invasions and threats to life. But what users want is entertain all the location based services without revealing their location information.

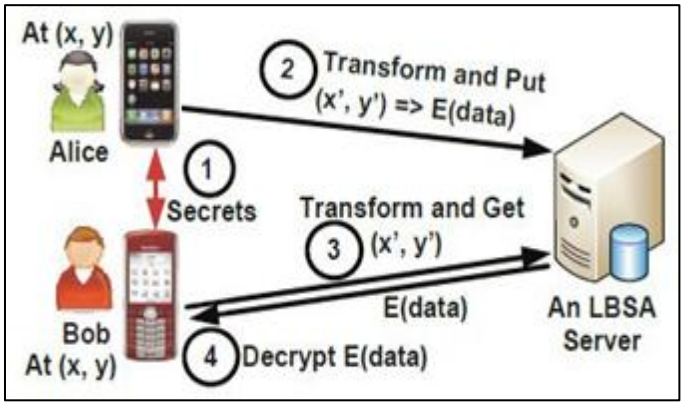

Fig. 1: Location Based Social Applications Basic Design

The existing system LocX [1] is used to avoid these limitations. In this method, before storing location in servers they are transformed to some other coordinates. So that another user cannot trace the path and also we can send the location to the

dishonest server. It improves the security and accuracy in LBSAs. It can use on any type of users query like point to point, nearest-neighbor etc.

The first step in LocX is sharing the key to users to whom we want to share our review. But in this phase the key is shared through mails or telephone. Also complex mathematical calculations are used to encrypt the location and data. LocX with dual encryption is used to improve the security. It contains a list of attributes and access policy.

The first section discuss about the related works based on Location Based Service Applications and their advantages and disadvantages. The next section discuss about the latest technique related to geo social applications named LocX and the system architecture of LocX followed by it is some drawbacks. To avoid these faults we proposed a technique in the next section LocX with dual encryption. And at last the performance evaluation of the existing system and the proposed system followed by conclusion.

II. RELATED WORK

The previous works for privacy preservation in LBS mainly focus on the following three dimensions: a) location privacy b) identity privacy c) query privacy.

One idea to preserve location is that send request from fake locations combined with the request from user's real world location [3]. The demerit related with this technique is that the number of false requests generated is very high and it will increase the cost. Another method is sending K-NN query from a fake location and linearly retrieve results like NN resources from the service provider until the user can locate the correct location [4]. Privacy is guaranteed because the service provider can only discover that the user is located within a region without learning the exact location. These techniques have been applied mostly for geo social applications performing k-NN spatial queries, and do not apply to proximity detection.

Next technique to preserve location is Location Anonymity in mobile geo social network by using Nearby Friend Alert [2][5]. To produce optimal grid overlay they apply the grid-and-hashing paradigm and multilevel grids for developing the detection accuracy .The main demerit is that it requires addressing issues.

Other solutions providing both location and identity privacy are used Private Information Retrieval (PIR) methods. The idea is to mapping the data transferred with the Service Provider, and to process the related query in an encrypted form, so that the server cannot retrieve the location and data. The techniques proposed in [6] are specially designed for NN queries, while [7] considers range queries over static resources, which is still not the proper setting for proximity detection. But it provides little bit overhead and computational cost to the existing system.

In the present paper we propose LocX that helps to protect user's privacy and also maintain full accuracy in local based social application (LBSAs). Hence, by distinguishing such location data through users social groups and further transformation can be used on location coordination. The coordinate are transformed to preserve locations, enhancing the task of server to perform queries on transformed location and data. The transformed locations are saved in different servers. The transformation is a secure one, since the secret is the key to the data, which knows only to the friends of the users. Also, they are more efficient, because LBSAs are least over- headed. So, these LocX lightweight built up application becomes quite fit for presently used devices. But little bit overhead occurs in this system.

III. EXISTING APPROACH

In LocX, there are mainly two servers. They are index server and data server. Index server is used for storing the encrypted location and data server for storing the encrypted location data. Fig.2. shows the LocX design

Suppose user A is at location (x, y) and want to write a comment about the place. First, he shares the secret key to the friends through any medium. Using the shared key he encrypts the location, and then saves to the index server through a dishonest proxy server. It is an intermediate server to send all the data. These proxies also see the transformed location that is encrypted with the index keys.

The index server cannot link to the users with location stored in it. The data is encrypted using the same index key and stored directly to the data server. Also, the location and data are stored in different servers it maintains unlink ability. This improves security. The main perceptive behind the security are of these reasons.

1) The index server does not find the actual coordinates because of the location transformation. To find the correct location, the third party needs to find the secret key they shared.

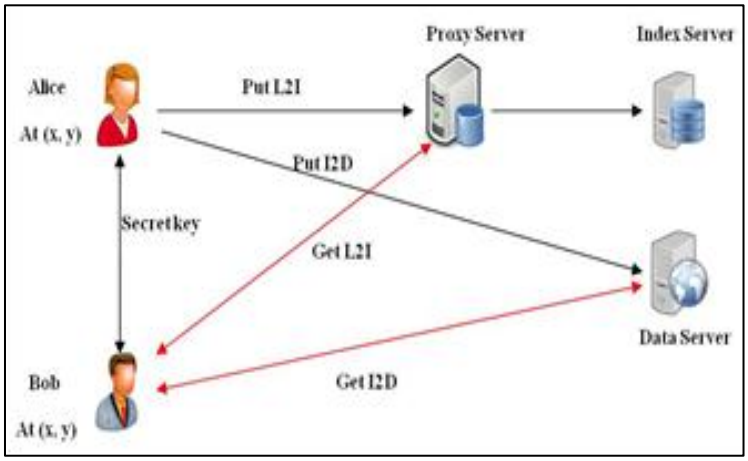

Fig. 2: LocX Design

2) The index server cannot link the various locations to the same user even though the hacker got the right key to decrypt because the location is transferred through the proxy server.

LocX design is shown in the Fig. 2. When Alice is at location coordinate (x, y), the steps involved in LocX are as follows.

1) The secret key is shared between the user Alice and Bob. Inexpensive symmetric keys are developed to map and decrypt the data.
2) L2I is the mapping from transformed location with E (i) where E(i) obtained by encrypting the secret key with a random index number. L2I is stored in proxy server. Proxy server is an intermediate server for requests from clients seeking resources from other servers. Then the L2I is saved in index server.
3) Next the location data is saved directly to the data server as I2D. I2D is the mapping from encrypted location and the index key.
4) Later Bob want to get the reviews shared by Alice about the location (x, y). This is done by using the right secret key and retrieves the L2I and identifies the location through proxy server.
5) At last using the same key he obtains the I2D from the data server and decrypts the data. Then it coupled with the corresponding location.

The index keys that are generated randomly are encrypted to E(i) before mapping with the location and then only it is stored in proxy server and then to the index server.

The main advantage of LocX from other basic LBSAs is that it does not rely on any trusted servers and thus location privacy and identity privacy is preserved. The location of the user and data related to it are stored in different servers. And also the location is encrypted with the transformed index. LocX provides high location privacy and not so easy to track information. But it is very expensive to implement. It gives more communication and computational overhead to existing systems. The inexpensive symmetric key is shared between the users. Also the key is shared through mails or messages. The third party can simply track the location if the user uses the same secret key yet again .But the location and the related data are saved in different servers the intruder cannot easily connect between them.

IV. LOCX WITH DUAL ENCRYPTION

To improve the security in LocX we use the scheme Dual Encryption. In a Dual System Encryption system both keys like cipher and private can use on one of two identical forms. By using encryption algorithm or system key's generation the cipher text and private is forms in normal form. These keys and cipher texts will perform alone in each system. And also it describes the keys like semi-functional keys and cipher texts. A semi-functional cipher text will be decrypt only by normal private keys and decryption will not succeed if one tries to decrypt a semi-functional cipher text with a semi-functional private key. Similarly, a semi-functional private key will be able to decrypt all usually created cipher texts. It is said to be asymmetric key encryption because it contains two types of keys .They are private key and semi functional key.

In encryption phase, location is mapped with the index key forming L2D and saved as encrypted file .The index keys used in encryption are random symmetric keys. At the same time, user's public key is encrypted and saved as Encrypted file encryption key (FEK). Later the encrypted file and encrypted FEK mapped together to form Encrypted file with FEK in header. The encrypted file is saved in proxy server and later to index server. Since it uses both private keys and user's public key it is said to be asymmetric cryptography. In asymmetric encryption, in which there are two related keys called key pair. A public key is made freely available to anyone who might want to send you a message and it is created by user itself and private key is kept secret. By using the same procedure all data's that are mapped by using the public key can only be decrypted, but by using the same private key. Any message that is encrypted by using the private key can only be decrypted by using the similar public key. But in symmetric keys it uses only private keys to encrypt, no public keys are used. The main advantage over LocX using dual encryption is the asymmetric key encryption so that it improves security and no third party can intrude into the server and track

the location of users. Similarly, the same technique can be used in the data's related to location and then saved in data server after dual encryption. The encryption phase in dual system encryption is shown in the Fig. 3.

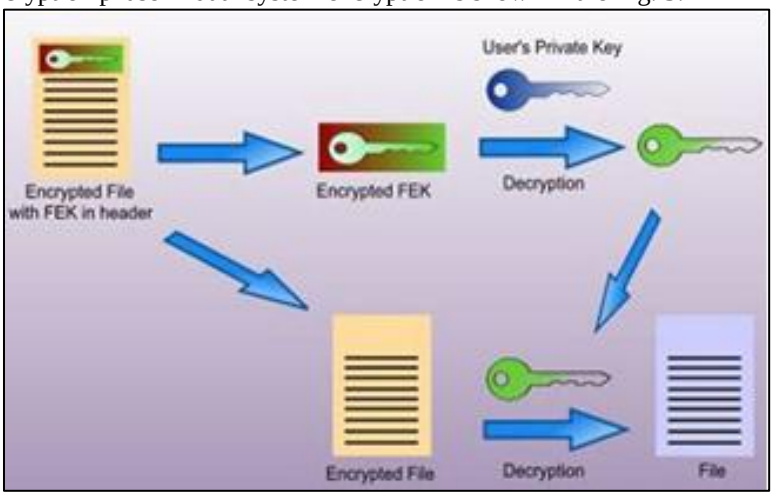

Fig. 3: Encryption phase in dual encryption

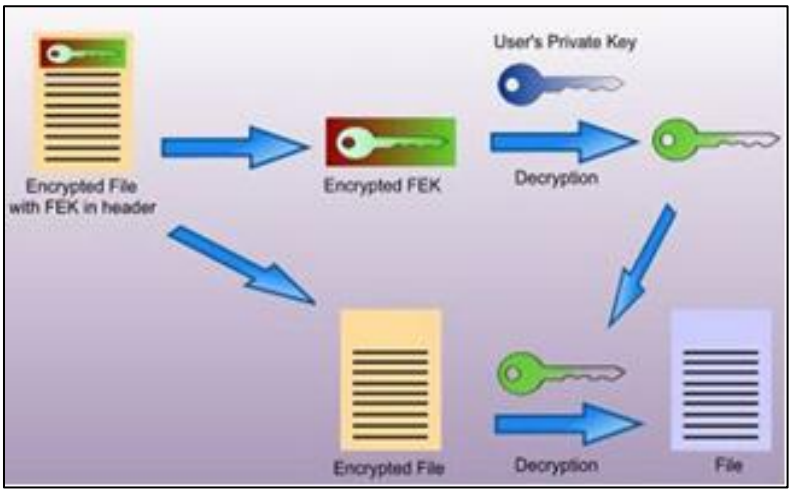

Fig. 4: Decryption phase in dual encryption

In decryption phase, the transformed location is given to the proxy server and gets the encryption file with FEK in header. It decrypts to FEK and encrypted file. Then using the private key that shared with the receiver B get the user's public key. With the public key it decrypts the encrypted file and get the correct location of the user A. Similarly, the same process is happen in the data server side. The I2D is given to the server. The decryption phase in dual system encryption is shown in the Fig. 4.

The system LocX with dual encryption goes through one additional phase compared to existing approach. But it improves security because a third party cannot decrypt the location and data without the intervention of the user.

V. PERFORMANCE ANALYSIS

There are many parameters to evaluate performance of LocX and LocX with dual Encryption like response time, encryption time, communication cost etc.

In fig.5 shows the processing time corresponds to their no of data points. LocX with dual encryption is high in processing time compared with LocX. In fig.6 shows the proposed and existing system encryption time with the number of data points. The result says that the time taken to encrypt the location and data is high in LocX with dual encryption because computational overhead and complexity in dual encryption is very high. Even though both the processing time and encryption time is high, the most important factor to improve is security. In LocX with dual encryption security is improved.

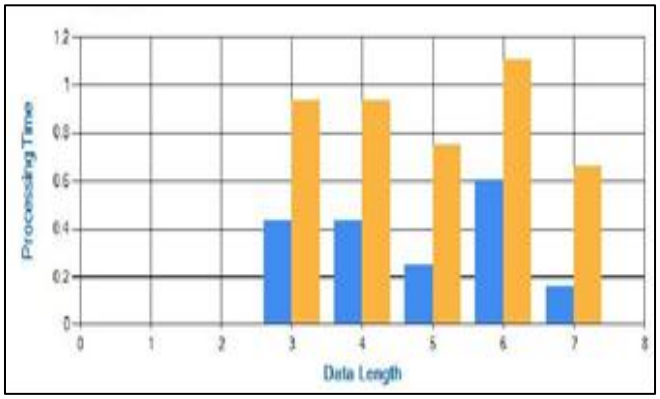

Fig. 5: Processing Time

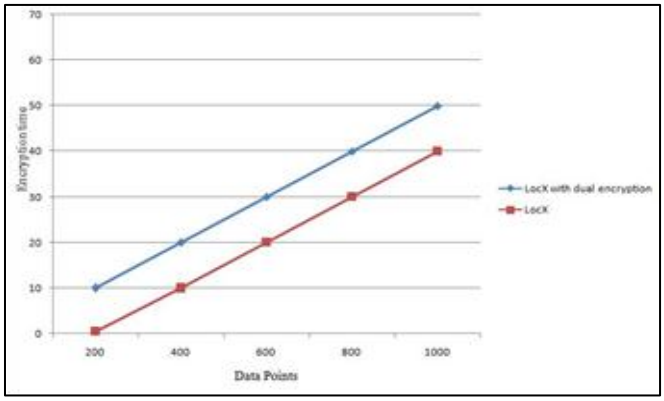

Fig. 6: Encoding Time

VI. CONCLUSIONS

LocX is the technique used to improve the location privacy in Location Based Service Applications (LBSAs). It uses many computational models to get accurate results. Also it uses the inexpensive symmetric keys to encrypt data. Hence runs efficiently on all mobile phones. LocX cause little bit computational and communication complexity to the existing systems. Hence LocX takes big steps towards location privacy for emerging large class of geo social application.
To improve the security we use the dual encryption scheme combined with LocX. In this scheme, asymmetric keys are used to encrypt the location. User's public key and a private key are used in encryption. In future user's privacy location in LocX with dual encryption is not so easy, it is very expensive. It goes through one additional phase compared to existing approach.

ACKNOWLEDGMENT

We express our sincere gratitude to God almighty for giving us the strength and blessing us with his grace. We also thank the faculty members and students of our college for their valuable support. We also express our heartfelt thanks to Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr EI Abbadi, Christopher Kruegel and Ben Y. Zhao, whose work inspired us to put forward this system.

REFERENCES

[1] Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr EI Abbadi, Christopher Kruegel and Ben Y. Zhao, "Preserving location privacy in geo-social applications," IEEE Transactions on Mobile Computing, vol:13, no. 1,pp. 159-173, January 2014.
[2] H. P. Li, H. Hu, and J. Xu. "Nearby Friend Alert: Location Anonymity in Mobile Geo-Social Networks." IEEE Pervasive Computing (PC), in press, 2013
[3] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh,"An anonymous communication technique using dummies for location-based services." In Proc. of the International Conference on Pervasive Services, pages 88–97, IEEE Computer Society, 2005.
[4] Man Lung Yiu, Christian S. Jensen, Xuegang Huang, and Hua Lu. SpaceTwist: "Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services." In Proc. of the 24th International Conference on Data Engineering, pages 366–375. IEEE Computer Society, 2008
[5] Hong Ping Li ; Hong Kong Baptist Univ., Hong Kong, China ; Haibo Hu ; Jianliang Xu, "Location Anonymity in mobile geosocial network," IEEE Computer Society on Pervasive Computing, vol:14, no. 4,pp. 62-70, December 2012.
[6] Stavros Papadopoulos, Spiridon Bakiras, and Dimitris Papadias,"Nearest neighbor search with strong location privacy" In Proceedings of the 36th International Conference on Very Large Data Bases (VLDB 2010),
[7] Ali Khoshgozaran, Cyrus Shahabi, and Houtan Shirani-Mehr. "Location privacy: going beyond k-anonymity, cloaking and anonymizers", Knowledge and Information Systems, 2010, to appear.