International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

Securing Location Privacy in Location Based Service Applications with ABE Scheme

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

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

***Abstract*— Location Based Service Applications (LBSAs) are becoming a part of our lives. Through these applications the users can interact with the physical world and get all data they want.eg; Foursquare .But it misuses it in many ways by extracting personal information of users and lead to many threats. To improve the location privacy we use the technique LocX .Here, the location and data related with it are encrypted before store in servers. So a third party cannot get the location from the server and the server itself cannot see the location. In addition, to reduce the computational complexity in the location transformation phase we introduce Attribute Based Encryption (ABE) method in LocX. So that the cost related with the transformation can be reduced.**

Keywords—Encrypt; Location Privacy; Threats

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. The users can interact with the physical world and get the details about the locations that their friends shared.

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.

The existing system to avoid these limitations is LocX. 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.

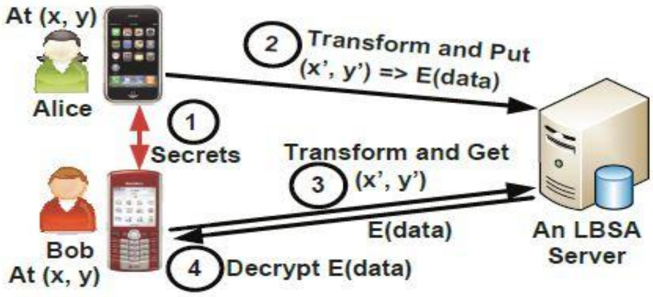

Fig. 1.Location Based Social Applications Basic Design

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. Attribute Based Encryption scheme is used to improve this drawback. It contains a list of attributes and access policy.

II. 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. LocX design is shown in the Fig. 2.

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 an dishonest proxy server. These proxies also see the transformed location.

The index server cannot link to the users with location stored in it. The data is encrypted using the same key and stored directly to the data server 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

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

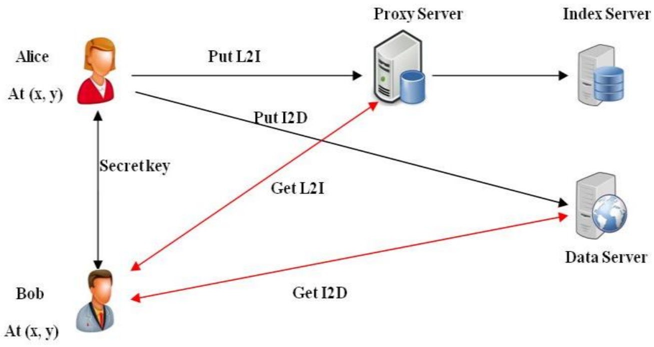

Fig. 2.LocX Design

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 used to encrypt and decrypt the data.

2. L2I is the mapping from transformed location with the 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 main advantage of LocX from other basic LBSAs is that it does not rely on any trusted servers.

II. PROBLEM DEFINITION

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 easily track the location if the user uses the same secret key again. But the location and the related data are saved in different servers the intruder cannot easily link between them. It is a difficult process.

IV. LocX WITH ABE METHOD

To reduce the calculation and complexity cost we use the scheme Attribute Based Encryption. It is an encryption technique where secret key depends on set of attributes and access policy. This policy gives permissions to users to decrypt the message and read the document. These attributes are generated based on user information. They are mainly two variants in ABE. They are as follows.

1. Key-Policy based ABE (KP-ABE)
2. Ciphertext Policy based ABE (CP-ABE)

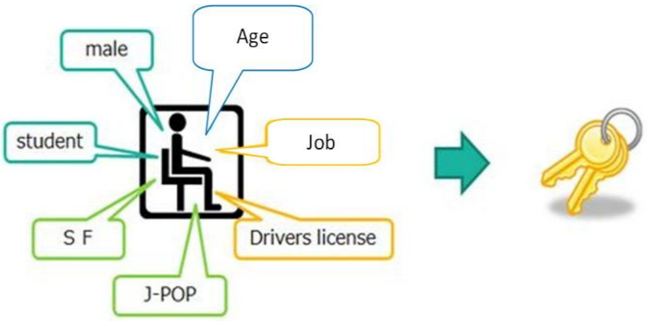

Fig. 2.Attribute Based Encryption Basic Design

The basic design of ABE is shown in the Fig. 3. In CP-ABE, the secret key is formed based on attributes and access policy is encrypted with the data. Suppose that the universe of attributes is defined to be {W, X, Y, Z} .User 1 receives a key W and X and user 2 to attribute Z. If the data is encrypted by the access policy ((W∧Y) ∨ Z), user A can decrypt the data but user B cannot decrypt. In KP-ABE, the secret key is generated based on access policy and attributes are encrypted with the data. We include the KP-ABE scheme in LocX mechanism.

Consider Alice is at location (x, y). Based on her personal information attributes are generated like age, job, place, address etc. Access policy can be expressed using Boolean operators like AND, OR. It can also be expressed in the form of predicates.

((Age ∧ Job) ∨ (Place ∧ Address ∧ Postal code))

This predicates can drawn in the form of access tree structure. It is given in the Fig. 4. The interior nodes contain the Boolean operators AND, OR and the leaf node contain the attributes. The user can change the access policy and corresponding to that access tree structure also changes.

Alice selects the access policy and shared with Bob. Attributes encrypted with the access policy forming E (k). L2I is the mapping from transformed location to E (k) and it is saved in proxy server. Similarly, I2D is the mapping from transformed data to the attributes. Later when bob is at location (x, y) he want to know the attributes related to Alice and also the access policy. Then only he can decrypt the L2I and I2D. It can be used in many complex access policies and reconstruct the secret by the user. It reduces the communication overhead in LocX.

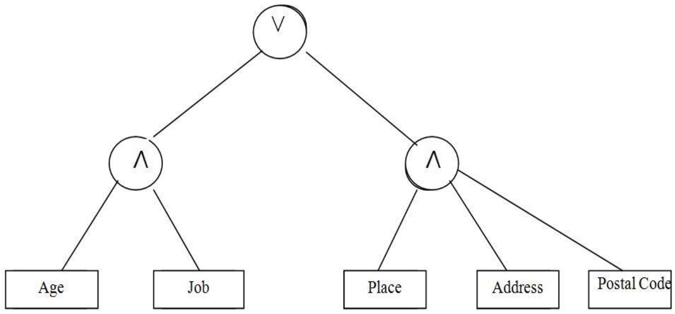

Fig. 4. Access Tree structure

V. CONCLUSION

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.

To overcome these faults we use the Key-Policy Attribute Based Encryption (KP-ABE) scheme. In this scheme, access policy is used as secret key and a list of attributes are used as index keys. Access policy can be change according to the users. Attributes are based on the user information. Thus ABE reduces the complexity in computation in LocX.

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]. B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection, "Computer, vol. 36, no. 12, pp. 135–137, 2003.

[3]. John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption," IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[4]. Goyal, V., Pandey, O., Sahai,A., Waters,B.(2006) "Attribute –based encryption for fine grained access control of encrypted data", ACM Conference on Computer and Communication Security, pp. 89-98.

[5]. Cheung,, L, Newport,C, (2007) "Provably secure Ciphertext police ABE", CCS 2007: Proceedings of the 14th ACM conference on Computer and Communications security, pp.456 -465, ACM Press, New York.