International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Review on Security in Geo-Social Applications through Preserving Location Privacy

Dhanashree Patil[1], Yogeshwari Borse[2]

[1] *Research Scholar, Department of Computer Engineering, SSBT's COET, Maharashtra, India*
[2] *Assistant Professor, Department of Computer Engineering, SSBT's COET, Maharashtra, India*

Abstract - *Location privacy protection is an imperative issue in our day by day life. The user needs to take care of their information. A large number of individuals collaborate with their surroundings through their companions and their suggestions. Without satisfactory protection, however, these frameworks can easily abuse, e.g., to track users or target them. In our busy calendar, we can't take care of our information. Along these lines, proposed system is to construct a utilization of safeguarding location privacy with the help of Distributed Systems. The paper presents dual encryption and compression model that gives significantly-enhanced location security without adding uncertainty into the query. The Proposed protocol gives a simple approach to secure our location information. Silent features of our location privacy protection framework are to give security to location data with enhancing the performance. This permits all location queries to be valuated effectively by the server, The proposed security system ensure that servers can't see or construe the real location information from the changed information.*

Key Words: *Location privacy, Dual encryption, location-based social applications, location transformation, compression.*

1. INTRODUCTION

Geo-social applications are used by millions of people, which gives an opportunity to interact, also sharing locations to unknown. However today's geo-social application have many privacy issues, which can easily misuse by an expert even a well-known person. Without privacy protection, hackers track users or target them. It will decrease the performance of the server and increase the time complexity[1].

The target scenarios bring out the following key requirements from an ideal location-privacy service.

• Strong location privacy: The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited.

• Location and user unlinkability: The servers hosting the services should not be able to link if two records belong to the same user or if a given record corresponds to a certain real world location.

• Location data privacy: The servers should not be able to view the content of data stored at a location.

• Flexibility to support point and nearest neighbor queries on location data.

• Efficiency in terms of computation, bandwidth to operate on mobile devices. The need for each of these requirements becomes more clear when to describing the related work.

2. LITERATURE SURVEY

G. Zhong, I. Goldberg, and U. Hengartner in [2] have briefly described that there are three participants in the Louis protocol: Alice, Bob and Trent. Alice and Bob are friends and Alice wants to know whether Bob is nearby. Alice considers Bob nearby if he is within a circle of some radius r centered around Alice. Alice informs Bob of r and Bob can refuse to participate in the protocol if he considers it to be too large. Trent acts as a third party and helps Alice and Bob decide whether they are nearby.

Another protocol is Lester, we do away with the need for Trent. However, this comes at some small costs. First, the information disclosure is now only one-way; that is, Alice learns about Bob s location, but not vice versa. Alice and Bob could, of course, run the protocol a second time, with the roles reversed, to mutually exchange information.

Another protocol is Pierre solves the problems with the Lester protocol and gives Bob more confidence in his privacy. On the other hand, if Alice and Bob are nearby, the Pierre protocol will inform Alice of that fact, but will give her much less information about Bob s exact location.

S. Mascetti, C. Bettini, and D. Freni in [3] have briefly described that Longitude is a work which adopts this technique. Longitude transforms locations coordinates to

prevent disclosure to the servers. In Longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends. Longitude eases privacy concerns by making it possible to share a user's location data blindly and allowing the user to control who can access her location, when and to what degree of precision. This is with the help of cryptographic algorithms and this can be adapted to mobile phones also. Here in the system model, it consists of a location-sharing service provider and the set of users registered with the provider. The provider store location along with some data. The user can determine which other users should view their data's. The security model assumes that the server is honest but curious about user's detailed location and information. The longitude protocol is based on proxy encryption. Here the user register with the service provider, the service provider provides them with some cryptographic elements. This can be saved safely in the user devices.

Reshmi K.U, Suja Rani M.S in [4] have briefly described that Location to index mapping is another approach towards location privacy of users. Here in this system the data and location are partitioned into two components and are stored on separate servers. The authorized person with the necessary credentials can only access the location information of the users. The location is stored in a server called as index server via another untrusted server called as proxy server. Proxy server is used in order for preventing the index server from uniquely identifying the client devices. Here the location information is transferred to another coordinate system and this is known as transformed location. Each user will be provided with an element which consists of a shift, a rotation angle, and an encryption key. Here in this system, this element will be shared with trusted friends circle.

Manu. P. Krishna and Jose Hormese in [5] have briefly described that in location transformation Transforming IDs is not enough to provide location privacy for users because some locations (e.g. homes) are strongly associated with user IDs and may thus cause an information leak. Location transformation, which is a crucial feature adopted for privacy. The main challenge in the development of suitable functions for location transformation is to keep the relative distance in each sub-dataset (the dataset obtained from the same agent) unaltered by the transformation in order to support location-based services. Possible transformation functions include scaling, rotating, translation, and their combinations.

B. Gedik and L. Liu describes in [6] have described that a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing. The model has two unique features. First, it provides a unified privacy personalization framework to support location k-anonymity for a wide range of users with context sensitive personalized privacy requirements. This framework enables each mobile node to specify the minimum level of anonymity it desires as well as the maximum temporal and spatial resolutions it is willing to tolerate when requesting for k-anonymity preserving location-based services (LBSs). Second, it devises an efficient message perturbation engine which runs by the location protection broker on a trusted server and performs location anonymization on mobile users' LBS request messages, such as identity removal and spatio-temporal cloaking of location information.

3. PROPOSED WORK

To improve the security in location points and data points it introduce dual encryption method in LocX. Asymmetric keys are used to encrypt the data with two keys public key and users private key.

3.1 Dual Encryption

In dual Encryption. Both keys are cipher and private can use on one of two identical forms in Dual Encryption. The cipher text and private is formed in normal form. Cipher texts and keys will perform alone in each system. And it describes the keys like semi-functional keys and cipher texts. Semi-functional cipher text will be decrypt normal private keys. Decryption does not succeed if one key tries to decrypt a semi-functional cipher text. Similarly, a semi-functional private key will be able to decrypt all usually created cipher texts. It is called as asymmetric key encryption because it contains two types of keys .These are private key and semi-functional key.

In encryption phase, location is mapped with index key forming and saved as encrypted file. The index keys used as random symmetric keys. At the same time, user's public key is encrypted. These key saved as Encrypted file encryption key (FEK). Then the encrypted file and encrypted FEK mapping together to form Encrypted file with FEK in the header. The encrypted file is saved in the proxy server and then saved to the index server. Since it uses both private keys and user's public key this is known as asymmetric cryptography. In asymmetric encryption, in there are two related keys called key pair. If anyone who

might want to send a message a public key is freely available. The private key is secret which is not freely available. By using same procedure all data's that are mapped by using the public key can only be decrypted, 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, public keys are not used. The main advantage of LocX using dual encryption is the asymmetric key encryption because 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.

In decryption phase, the transformed location is given to the proxy server. It gets the encryption file with FEK in the header. It decrypts to FEK and encrypted file. Then using the private key that shared with the receiver get the user's public key. By using the public key it decrypts the encrypted file and gets correct location of the user. Similarly, the same process is occurs in the data server side.

3.2 Compression

When the user wants to share some information about any location retrieves the co-ordinates (x,y) of that location from the GPS system. Then it uses secret rotation angle and shift, he will transform those co-ordinates say (x', y'). A random number generator is used to generate the index. It is encrypted with the secret key. Then the transformed co–ordinates along with encrypted index will be saved on to the index server. The data corresponding to this location is encrypted. It uses the secret key. This data is again compressed. For improving the performance of review retrieval to the data server we can use the compression mechanism. This mechanism compresses the reviews and stores it to the data server.

When User's friend wants to access the reviews for the specified location again he transforms the co-ordinates and sends the query to the index server. Then he retrieves the index by using the secret key. After retrieving the index a separate query will be fired on to the data server to fetch the review. The review will first decompress and then decrypted with the same secret key.

In this way, the recommendations can be securely communicated within the user's social circle without exposing his location to the outside world.

Fig-1 shows the overview of system operations.

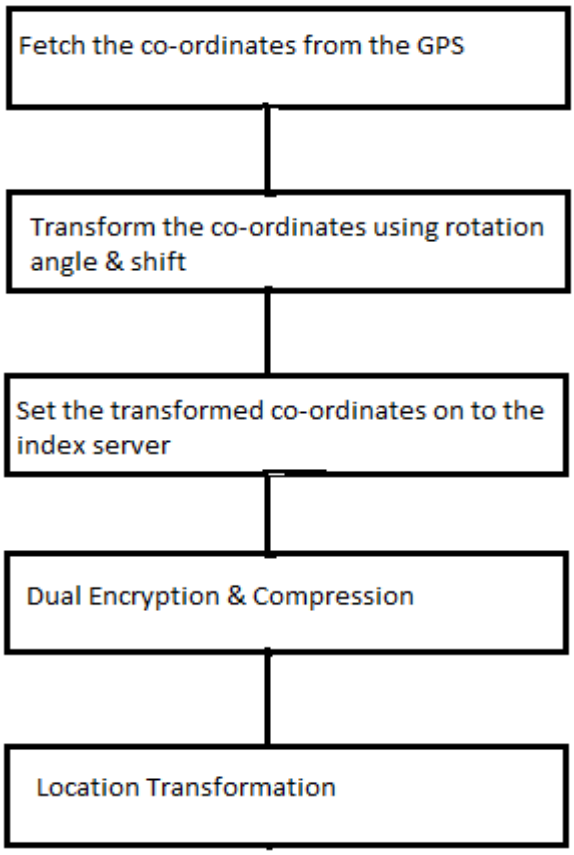

Fig-1: Overview of System Operations

4. CONCLUSIONS

This paper tells about the study of different protocol and technique in location privacy. It improves the accuracy. It reduces the little computational and communication overhead to existing systems. It maintains the unlinkability between different queries is critical. It reduces the system complexity by sharing the secret key. In future, different techniques will be used to improve the performance of existing techniques.

REFERENCES

[1] Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, "Preserving location privacy in Geo-Social applications", IEEE Transaction on Mobile Computing Vol. 13, No: 1, January 2014.

[2] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, Lester and Pierre: Three protocols for location privacy", in Proc. of PET, 2007.

[3] S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized privacy-preserving computation of users proximity", in Proc. of SDM, 2009.

[4] Reshmi K.U, Suja Rani M.S, "A Survey on Preserving State of Location Privacy in Geo Social Application", Vol. 3, Issue 1, January 2015.

[5] Manu. P. Krishna and Jose Hormese, "Survey on pre--serving location privacy in Geo-social application", Vol. 3, Issue 4, April 2015.

[6] B. Gedik and L. Liu, "Location Privacy in Mobile Syste--ms: A Personalized Anonymization Model", Proc. IEEE 25th Intl Conf. Distributed Computing Systems, 2005.