International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

Privacy Preserving Location Query Service

P.Sampath Kumar, K. RAJENDRA PRASAD, A. SOUJANYA, Ch. SRIKANTH

Student, M.Tech CSE Dept.,
Institute of Aeronautical Engineering,
Hyderabad-500043, Telangana, India.

Professor & HOD, CSE Department
Institute of Aeronautical Engineering
Hyderabad -500043, Telangana, India

Assistant Professor CSE Dept.,
Institute of Aeronautical Engineering,
Hyderabad-500043, Telangana, India.

Assistant Professor CSE Dept.,
Institute of Aeronautical Engineering,
Hyderabad-500043, Telangana, India.

Abstract - *Location-Based Service (LBS) is a service that provides the information and the number of uses in social network as in security that is accessible through mobile network and finds the geographical location of the mobile device using that location .It is used in different contexts such as entertainment, indoor object search, health. One of its most powerful aspects is that it provides spatial patterns. It evolved from simple based service models to complex tools for implementing any location based service model or facility. The important thing about this service is the data about subscribers location is owned and controlled by the network operators, including mobile carriers and mobile content providers. The privacy of the user in different distributed networks is considered by using location-based query algorithm efficiently. It proposes an algorithm which offers the location query services simultaneously to multiple users thus improving the performance of the server and satisfy the request of users location.*

1. INTRODUCTION

The Location Based Services started emerging with the development of wireless communication technology in mobiles recently.Temporal and Spatial information of users is made using the users location information.The main important problem of the location based services is to preserve the privacy of the users location..It canbe achieved using the anonmity on the location based services.It is an effective method to effective method to prevent the quasi identifiers of the users.The k-anonymity model is introduced to find the problem of preserving the location privacy of the users. Balancing the quality of query services and providing the privacy protection is one of the important issue in the distributed networks for the privacy-preserving location-based services . In this paper, an efficient privacy-preserving location-based query algorithm is proposes which uses parallel searching technique to improve the efficiency of the unknown server, which not only protects the location privacy of the user but also obtain the location query services. Location indexes and parallel searching in the distributed networks uses an efficient privacy-preserving location-based query algorithm. Many people carry handheld devices each and every day equipped with localization capabilities thus allowing the users to access a wide variety of online services. Location-based services provide users with various functionalities like access to information (weather forecast, road traffic, to find friends or points of

interests in the neighborhood and even to play social games). The user must communicate to the LBS her exact current location to obtain desired service. It raises severe privacy problems due to the knowledge LBSs are able to know about users location. The easiest way is to gather built access control in light of distributed areas to a large portion of uses received that determine a gathering of client who can or can't see them . Social networking site Flickr, Face book and Google+ just let users pick all users, neighbors, companions or family to permit the right to gain entrance to the areas, and provides SNS to help custom gatherings to determine the open client bunches. There are some applications that are much more awful. They don't even offer bunch decisions to the clients, rather, they just ask users whether they need to uncover or not . Clients can just determine a gathering of clients who can or can't get to the data. In this way, a finegrained protection control executable on encoded area information is required to encourage the LBS and its business market further.

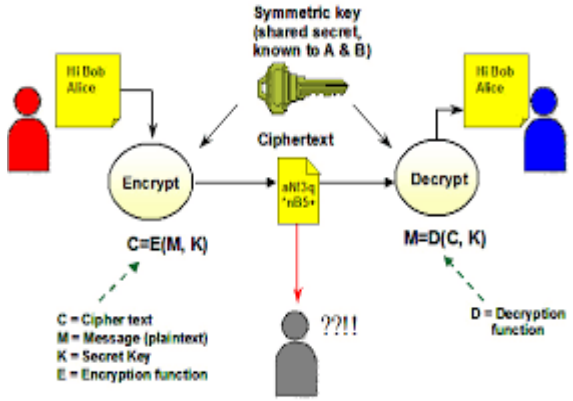

Fig1: Carolyn and Mathews Location based Services

With this solution, Mathews can just send Carolyn a single aggregate key thorugh an email in secured manner. Carolyn can download the photographs that are encrypted from Mathews Dropbox space and later utilize this aggregate key to decrypt these photographs which are encrypted. The situation is shown in above figure.

Using the standard model the developments can be demonstrated securely. To the best of our insight, our aggregation mechanism in KAC has not been explored.

2. PRELIMINARIES

PRIVACY-PRESERVING LOCATION QUERY PROTOCOL (PLQP)

In this paper various cryptographic techniques are used.

Attribute-Based Encryption

In this section, the identity of a user is viewed as a set of attributes. Key Policy Attribute Based Encryption and Ciphertext-Policy Attribute-Based are types of Attribute-Based Encryption System.It specifies the encryption policy in the decryption key, and the CP-ABE specifies the policy in the ciphertext.

Homomorphic Encryption

Homomorphic Encryption preserves decryptability allowing direct addition and multiplication on ciphertexts .

Enc(m1).Enc(m2)=Enc(m1+m2) ;

Enc(m) -for the ciphertext of m

Partially Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE) are two types of Homomorphic Encryption.Some fundamental suppositions preserving location privacy while achieving utility from it is still a challenging question now. This project tackles this non-trivial challenge by designing a suite of novel fine-grained Privacy-preserving Location Query Protocol (PLQP). This allows multilevels of location query on encrypted location information for different persons, and it is efficient enough to be applied in smartphones

. **Fig 2: Architecture of LBS.**

Functional Encryption

Functional Encryption is a new encryption scheme that is recently proposed after the Attribute-Based Encryption. They proposed the terminology Functional Encryption in 2011.In the today's fast growing world, Functional Encryption is an encryption scheme such that a key holder can learn a specific function of the data based on the cipher text, but nothing else about the data use of internet. In Functional Encryption, encrypted can specify a function for the key such that each decryption result is the corresponding function of the plaintext. Service providers require user's current geographical position to query their location. The main objective of the present work is to develop a system that preserves the location privacy of the each individual. This can be achieved by simulating locally cloak algorithm and globally cloak algorithm for Manhattan and Waypoint mobility model.

The main objective of the current work is to develop a system that preserves the location privacy of the concerned individual. This objective is achieved by simulating locally cloak algorithm and globally cloak algorithm using NS - 2.34 environments. An approach that combines obfuscation and anonymization to ensure both location and anonymity privacy for mobile agents is presented. When sender and receiver [sink node] communicate in a clique obfuscates (masks) its current position by providing a rectangle instead of a point as its location. During simulation it is seen that GCA algorithm generates minimum bounding box of size LCA. Aga in it is seen that more the node density, the GCA algorithm maximizes the bounding box size, which results in maximum location privacy for secure communication. The value of k-anonymity increases then GCA area also in cases up to certain level.

```
double xSqr = Math.pow(xDiff, 2);

double yDiff = d2-d4;

double ySqr = Math.pow(yDiff, 2);

double output= Math.sqrt(xSqr + ySqr).
```

3.MODULES DESCRIPTION

Fine-Grained Access Control: This protocol allows users to maintain a condition instead of a group and exert access control over the users who satisfy this condition. It is more scalable as users can simply specify a new condition for new privacy setting instead of picking many users to form a new group. Also, it is more user friendly because users themselves do not clearly know which of their friends should or should not access the information most of time.

Multi-leveled Access Control: This protocol also supports semi-functional encryption. It means the protocol enables users to control to what extent (or level) others can learn their location. The lowest level corresponds to nothing, and the highest level corresponds to one's exact location. Levels between them correspond to indirect information about one's location.

Privacy-Preserving Protocol: In our protocol, each and every location information is encrypted. The queries are processed based upon cipher texts. A location publisher's friends can learn nothing but the result of the location query, which is secured with the location publisher's control. In

addition to this, since every location is encrypted, even the server who stores location information does not learn anything from the cipher text.

Euclidean Distance: Simply, we assume the ground surface is a plane, and each and every users location is mapped to an Euclidean space with integer coordinates (with meter as unit). Everyone's location can be expressed as a tuple of coordinates representing a point in a grid partition of the space.

4. EXPERIMENTAL RESULTS

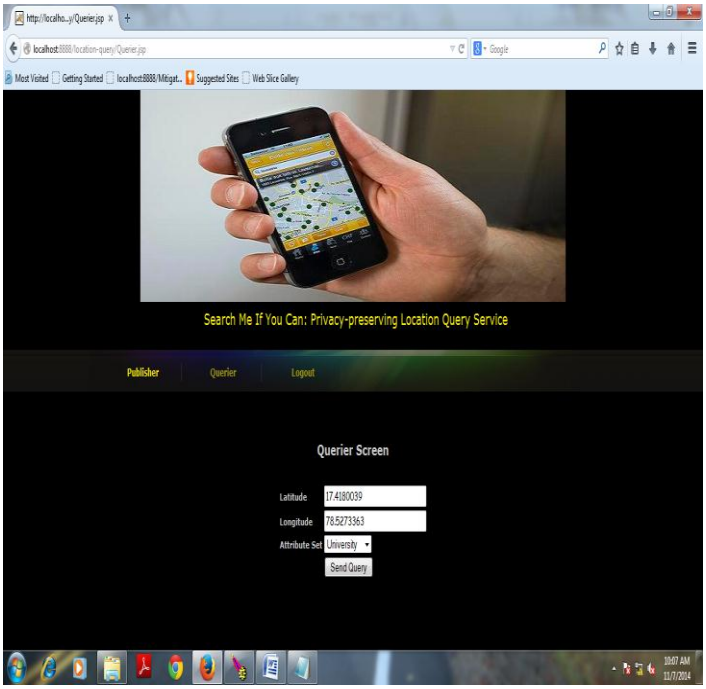

Fig 3: User enters the details where he is at present location

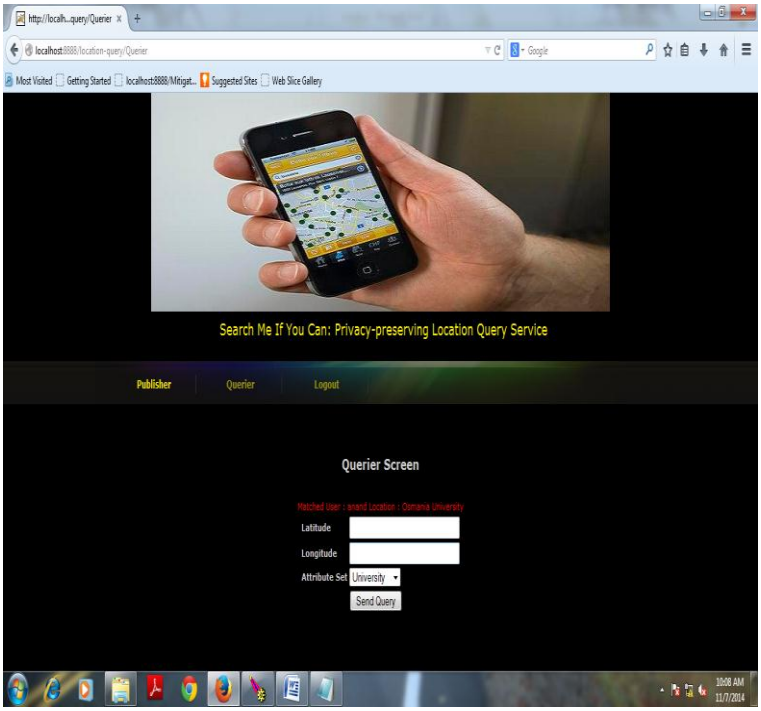

Fig 4: If any user is available in the given location range user will be displayed.

5.CONCLUSION

This project proposes a fine-grained Privacy-preserving Location Query Protocol (PLQP), which successfully comprehends the privacy and gives different area based inquiries.. The PLQP uses novel separation calculation and examination convention to execute semi-practical encryption, which backs multi-leveled access control and used CP-ABE as subsidiary encryption scheme to make access control be more fine-grained. We additionally directed investigation assessment to demonstrate that the execution of our convention is material in a genuine versatile system.

ACKNOWLEDGEMENT

We thank our HOD "**Prof. K. RAJENDRA PRASAD**" for giving us the eminent facilities to perform my Project work. I am obliged to of CSE department, IARE for their timely help and support.

REFERENCES

[1]. C. Dwork, F. McSherryand L. Kulik, "Privacy via distributed noise , 2006.

[2]. Z. Lan, K.-B.Liu, Y.-H. Jiang, X.-Y. Li, Y. Liu, and P.Yang, "Montage: Combine Frames with Movement Continuity for Realtime Multi-User Tracking," in Proc. Of IEEE INFOCOM, 2014 .

[3]. C. Bettini, X. Wang, D. Wei, V. Dave, L. Qiu, and Y. Zhang. Secure Friend Discovery in Mobile Social Networks 185–199, April 2005.

[4]. M. Andres, N. Bordenabe The new casper: query processing for location services without compromising privacy, Proc. of the 2013 ACM SIGSAC Conference on Computer & communications security," in Proceedings of the 32nd, IIT Bangalore.

[5]. Z. Lan, K.-B.Liu, Y.-H. Jiang,An Efficient Sharing of personal Health records Using DABE in Secure Cloud Environment,International Journal of Advanced Research in Coumputer Engineering & Technology, Vol 2, Issue 3,March 2013.

[6]. Cheng-Kang CHU, "An Anonymous Communication Technique Using Dummies for Locationbased Services", Proceedings of IEEE International Conference on Pervasive Services, Singapore Management university. (2005); ICPS.

[7]. Baojiang Cui,Zheli Liu,Key-Aggregate Searchable Encryption(KASE) for Group Data Sharing Via Cloud Storage,IEEE Transactions on Computers,Vol 6,Jan 2014.

[8]. K.manohar,R.AnilKumar, Key-Aggregate Searchable Encryption for Group Data Sharing Via Cloud Storage,International Journal of Computer Engineering in Research Trends,Vol 2,Issue 12,Dec 2015,PP.1132-1136.

[9]. Vanya Diwan, Shubhra Malhotra,Rachna Jain, Cloud Security Solutions: comparison among various Cryptographic Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, New Delhi, India.