International Journal of Science Engineering and Advance Technology
IJSEAT

Efficient Tree Structured Algorithm For Providing Confidentiality Of Location Data To Minimize Communication Overhead In LBS Services

[1] K.Parvati, [2] P.RamaKrishna
1,2Dept. of CSE, Kakinada Institute of Engineering and Technology,
KKD-YANAM Road Corangi, EG Dist AP-533461, India

ABSTRACT:

We present an effective and protection safeguarding polygons spatial inquiry structure for area based administrations, called Polaris. With Polaris, the LBS supplier redistributes the encoded LBS information to cloud server, and the enrolled client can question any polygon range to get precise LBS results without revealing his/her inquiry data to the LBS supplier and cloud server. Proficient uncommon polygons spatial inquiry calculation over ciphertext is developed dependent on an enhanced homomorphic encryption innovation over Composite request gathering. With SPSQ, Polaris can look re-appropriated scrambled LBS information in cloud server by the encoded demand, and react the scrambled polygons spatial question results precisely.

KEYWORDS: Polaris, spatial query, encrypted.

INTRODUCTION:

LOcation-based services (LBS), which are a general class of PC program-level administrations that utilization area information to control highlights [1]– [4], are widly utilized in an assortment of settings [5]– [7], for example, budgetary administrations, transport, relaxation travel, social insurance, car, promotion organizations, and so forth. Clients just need to include a geological position, at that point the LBS can give the most significant data to them. For instance, when an individual is going in a bizarre place, LBS can encourage him/her find a few spots, for example, vacation spots, hotel,the closest healing facility, etc. For giving more adaptable and advantageous LBS, polygons spatial question has been proposed and pulled in significant intrigue as of late. We consider the accompanying situation as appeared in Fig.1, people may lean toward the healing center A to B, in spite of the fact that the direct separation from the previous is more remote than the last mentioned. Thinking about the genuine street circumstance, clearly going healing center An is more helpful and quicker than B. Despite the fact that polygons spatial inquiry can give LBS all the more helpfully, inferable from the affectability of clients' area data, there are as yet numerous difficulties lying ahead in the advancement of LBS framework [8]– [10].

LITERATURE SURVEY:

THE AUTHOR, Panos Kalnis (ET .AL), AIM we present a structure for anticipating area based character deduction of clients who issue spatial inquiries to area based administrations. We propose changes dependent on the entrenched K-secrecy idea to figure correct responses for range and closest neighbor look, without uncovering the inquiry source. Our techniques upgrade the whole procedure of anonymizing the solicitations and preparing the changed spatial questions.

THE AUTHOR, R. Zheng **(ET .AL), AIM**. we propose a mechanism based on locality-sensitive hashing (LSH) to parcel client areas into gatherings each containing in any event K clients (called spatial shrouds). The instrument is appeared to protect both area and K-obscurity. We at that point devise a productive calculation to answer kNN inquiries for any point in the spatial shrouds of self-assertive polygonal shape.

PROBLEM DEFINITION:

Prior strategies like k-Anonymity procedure shrouding system and homomorphic encryption methods are presented in LBS.

k-Anonymity guarantees that a client can't be related to a likelihood something like 1/k through separating client area into gatherings each containing at any rate k clients.

Shrouding strategy is widely used to keep the divulgence of client's information through obscuring client area into a shrouded spatial locales.

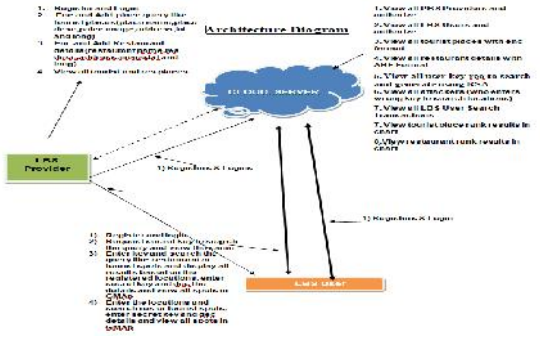
PROPOSED APPROACH:

Proposed Polaris gives a protection saving polygons spatial inquiry system for LBS. With Polaris, clients can set the question run freely and keep his/her inquiry polygons mystery from the LBS supplier and cloud server.

Polaris presents an enhanced homomorphic encryption innovation over composite request gathering and hash esteem successions.

Just enrolled clients are permitted to inquiry and get the alluring LBS information

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

LBS PROVIDER

In this module, LBS Provider has to register to cloud server and cloud server authorizes the data provider login. The provider adds the place details , restaurant details with its name, description, image, address, latitude and longitude and encrypts the details and uploads to cloud.

CLOUD SERVER

Cloud server will authorize both LBS provider and the LBS user, and can view all uploaded tourist and the restaurant details in ABE format. Generates the key to search, using RSA requested by the users. View the attackers who give wrong key to search locations, and the Corresponding transactions.

LBS USER

In this module LBS user has to register and login, and the user is authorized by the cloud server, user will request secret key to search the query from the cloud server. And the user can only search the queries only with the generated key by the cloud, and after the search results the user has to enter the key to decrypt the same. Search is done based on two criteria 1) keyword and 2) location. And view the place on the google map.

ALGORITHM:

SPECIAL POLYGONS SPATIAL QUERY ALGORITHM:

INPUT:AU,LP,LU,CS

STEP1:AU generates system parameters and publishes it to LP AND CS.

STEP2:LP get the location information and compute location index.

STEP3:LP encrypt location information and outsource to CS.

STEP4:LU is registered by LP.

STEP5:LU choose query points and encrypt those query points .

STEP6:based on LU query points signature is generated.

STEP7:after signature verification response is generated by CS

STEP8:finally query results are decrypted.

SS-TREE ALGORITHM:

INPUT:NODES,QUERY TOKEN,NODESLIST

STEP1:search starts from root node.

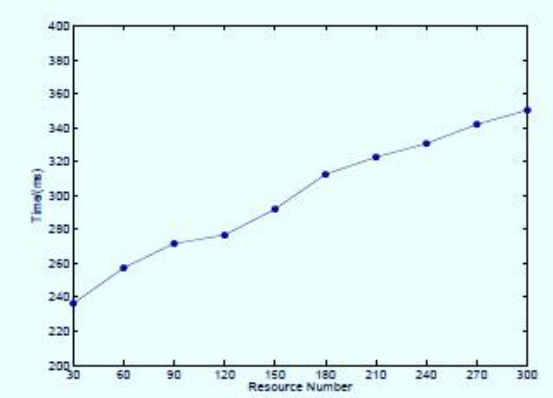
STEP2: If a nonleaf node's area intersects with the query area

STEP3: all children of the node will be scanned.

STEP4: Otherwise, all descendant nodes of this nonleaf node are skipped.

STEP5: Detecting circular area intersection and matched records are based on our spatial query algorithm for inner product range.

RESULTS: It is obvious that the computation overhead of LP increases linearly as the number of resources increase.



Computation cost of LP

CONCLUSION:

We have proposed a gainful and security ensuring polygons spatial inquiry framework for region based organizations, named Polaris. In perspective of an improved capable homomorphic encryption development over composite demand assembling, the proposed Polaris can achieve question polygons security assurance and mystery of LBS data. Specifically, for a LBS question request from a selected LU, the LBS request execution is direct performed over ciphertext on CS without unscrambling, and the result of LBS request must be decoded by LU. Along these lines, LU can get correct LBS question result without revealing his/her request information. Positive security examination exhibits its security quality and insurance defending limit, and wide preliminaries are directed to demonstrate its efficiency.

REFERENCES:

[1] D. L. Goroff, "Balancing privacy versus accuracy in research protocols," Science, vol. 347, no. 6221, pp. 479–480, 2015.

[2] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models," Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 393–413, 2014.

[3] H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," 2015.

[4] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," Wireless Communications, IEEE, vol. 22, no. 4, pp. 74–80, 2015. IEEE Internet of Things Journal,Volume:4,Issue:2,Issue Date:April.2017 10

[5] H. Zhu, T. Liu, G. Wei, and H. Li, "Ppas: privacy protection authentication scheme for vanet," Cluster computing, vol. 16, no. 4, pp. 873–886, 2013.

[6] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 8, pp. 2053–2064, 2014.

[7] H. Zhu, X. Liu, R. Lu, and H. Li, "Efficient and privacy-preserving online medical pre-diagnosis framework using nonlinear svm."

[8] L. Li, R. Lu, and C. Huang, "Eplq: Efficient privacy preserving location-based query over outsourced encrypted data," Internet of Things Journal, IEEE, vol. PP, no. 99, pp. 1–1, 2015. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7206527

[9] J. Shao, R. Lu, and X. Lin, "Fine: A fine-grained privacy-preserving location-based service framework for mobile devices," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 1452–1461.

[10] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An efficient privacy-preserving location based services query scheme in outsourced cloud," Vehicular Technology, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2015. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7327242

[11] S. Landau et al., "Control use of data to protect privacy," Science, vol. 347, no. 6221, pp. 504–506, 2015.

[12] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," Science, vol. 347, no. 6221, pp. 509–514, 2015.

[13] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557–570, 2002.

[14] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," Knowledge and Data Engineering, IEEE Transactions on, vol. 19, no. 12, pp. 1719–1733, 2007.

[15] K. Vu, R. Zheng, and L. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 2399–2407.

Ms.K.Parvati is a student of Kakinada Institute of Engineering and Technology,korangi.presently she is pursuing his M.Tech (Computer Science and Engineering) from this college and she received his B.Tech from Srinivasa Institute of Engineering and Technology, cheyyeru affiliated to JNTU,kakinada in the year 2016..

Mr.P.RAMAKRISHNA,well known author and excellent teacher.He working as Associate professor Department of M.Tech.He has 7years of teaching experience in Kakinada Institute of Engineering and Technology,korangi.