International Journal of Advanced Technology and Innovative Research

www.ijatir.org

ISSN 2348–2370
Vol.11,Issue.01,
January-2019,
Pages:22-25

A Secure Location Based Service Search in Cost Efficient Cloud Environments

MANGALAGIRI NARMADHA[1], R. M. MALLIKA[2]

[1]Research Scholar, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, Nellore, AP, India,
E-mail: devinarmadha786@gmail.com.

[2]Associate Professor & HOD, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, Nellore, AP, India,
E-mail: mallika.521@gmail.com.

Abstract: The growth of mobile devices and the development of wireless communication technique, location-based services (LBS) have made our life more convenient, and the polygons spatial query, which can provide more flexible LBS, has attracted considerable interest recently. However, the flourish of polygons spatial query still faces many challenges including the query information privacy. In this paper, we present an efficient and privacy-preserving polygons spatial query framework for location-based services, called Polaris. With Polaris, the LBS provider outsources the encrypted LBS data to cloud server, and the registered user can query any polygon range to get accurate LBS results without divulging his/her query information to the LBS provider and cloud server. Specifically, an efficient special polygons spatial query algorithm (SPSQ) over cipher text is constructed, based on an improved homomorphic encryption technology over composite order group. With SPSQ, Polaris can search outsourced encrypted LBS data in cloud server by the encrypted request, and respond the encrypted polygons spatial query results accurately.

Key Words: Location Based Services, Privacy Preserving, Query Processing.

I. INTRODUCTION

Location-based services (LBS), which are a general class of computer program-level services that use location data to control features, are widely used in a variety of contexts, such as financial services, transport, leisure travel, healthcare, automotive, ad agencies, etc. Users only need to input a geographical position, then the LBS can provide the most relevant information to them. For providing more flexible and convenient LBS, polygons spatial query has been proposed and attracted considerable interest recently. Although polygons spatial query can provide LBS more conveniently, owing to the sensitivity of users' location information, there are still many challenges lying ahead in the development of LBS system. For instance, plenty of users' sensitive information could be easily analyzed and revealed by the LBS provider. If those sensitive information is obtained by an attacker who could determine users' location and track them, this will open up many computer-aided crime possibilities. Therefore, how to design a secure and efficient privacy-preserving polygons spatial query framework for LBS system has attracted considerable interest recently. To address these challenges, the k-Anonymity technique, cloaking technique and homomorphic encryption techniques are introduced in LBS. Specifically, k-Anonymity ensures that a user cannot be identified with a probability at least 1/k through parting user location into groups each containing at least k users.

Cloaking technique is extensively used to prevent the disclosure of user's data through blurring user location into cloaked spatial regions. However, both k-Anonymity technique and cloaking technique bring heavy communication overhead to user side, which lead to much energy consumption on the mobile device. In addition, traditional homomorphic encryption techniques, which can achieve data operations over encrypted data with low communication overhead, ensure that the probability of a user being identified is very low. However, most of them require massive resource-consuming computation, which makes them not quite suitable for the mobile device, either. In this paper, we propose an efficient and privacy-preserving polygons spatial query framework for location-based services, called Polaris. With Polaris, the LBS provider can outsource their encrypted data to the cloud server, and users can query any polygon range to get accurate encrypted LBS results in cloud server with encrypted query information. In addition, the proposed framework is characterized by protecting the users' query information privacy from the LBS provider and cloud server, and keeping LBS provider's sensitive data secret from the cloud server.

II. BACKGROUND WORK

The range query privacy has gained great interest in recent years, and we briefly review some related to ours. Most previous works on location based services adopt the k-Anonymity to ensure user's privacy. Specifically, Kalniset al. presented a framework for preventing location-based identity inference of users who issue spatial queries to Location Based Services, whose transformations based on the well established k-anonymity concept to compute exact answers for range and nearest neighbor search, without revealing the query source. Ku et al. provided network distance spatial query solutions algorithms for answering nearest neighbor queries and range queries on spatial networks without revealing private information of the query

initiator by utilizing k-anonymity mechanisms. Vu et al. proposed a mechanism based on locality-sensitive hashing (LSH) to partition user locations into groups each containing at least k users (called spatial cloaks),which is shown to preserve both locality and k-anonymity, and devise an efficient algorithm to answer KNN queries for any point in the spatial cloaks of arbitrary polygonal shape. However, k-Anonymity ensures that a user cannot be identified with a probability at least 1/k. Although the adversary does not infer the actual location in general, the location information will be leaked if k users' locations were in the same place or in a sensitive region, and it brings heavy communication overhead to user.

Cloaking technique are extensively used to prevent the disclosure of user's data through blurring the user location into a cloaked spatial regions. Mokbel et al. presented a framework in which user can entertain location based services without revealing their location information by blurring users' exact location into cloaked area. Different only focus on handling rectangular cloaked regions, Liu et al. proposed a new convex hull of polygon(CHP) algorithm for nearest-neighbor queries using a polygon cloaked area. Ngo et al. introduced a new location privacy ware nearest-neighbor query processor that provides efficient processing of complicated polygonal and circular cloaked regions, by proposing the Vertices Reduction Paradigm and the Group Execution Agent. However, instead of returning exact answers to the user, the above privacy framework using cloaking technique returns a list of candidate answers according to the cloaked users or cloaked area which brings heavy communication overhead to user side. What's more, those schemes provided LBS with plaintext in server, which is not suitable for outsourced environment. Homomorphic encryption is a usual method to achieve data operations over encrypted data without decrypting it, which can be used for outsourced environment. Ghinita et al. protected the location privacy of users by encrypting location data using private information retrieval (PIR) protocols and devise cryptographic protocols that privately evaluate whether a point is enclosed inside a rectangular region or a convex polygon and provide solutions for exact NN queries with Paillier's homomorphic encryption.

Mu et al. proposed a novel approach that allows a mobile user to define an arbitrary convex polygon on the map and test whether locations are located therein. They employed a secure two-party computation protocol which is based on Pailler homomorphic cryptosystem. However, most of homomorphic encryption schemes require massive resource-consuming computation, which makes them not quite suitable for providing efficient LBS service. Different from above works, our proposed Polaris framework aims at the efficiency and privacy issues, and based on an improved homomorphic encryption technology over composite order group, we develop an efficient privacy-preserving spatial range query scheme for polygon in outsourced cloud. In particular, the proposed Polaris framework can easily be implemented in the smart phone and cloud server, and the processing of spatial range query is just needed in the cloud server. The computation costs in both smart phone and cloud server are acceptable.

III. PROPOSED METHOD

A. System Model

The system model focus on how to provide an accurate and efficient polygons spatial query over outsourced cloud server without divulging the LBS data and the query information, and it consists of four parts: Authority (AU), LBS provider (LP),LBS User(LU), and Cloud Server(CS), as shown in Fig.1.

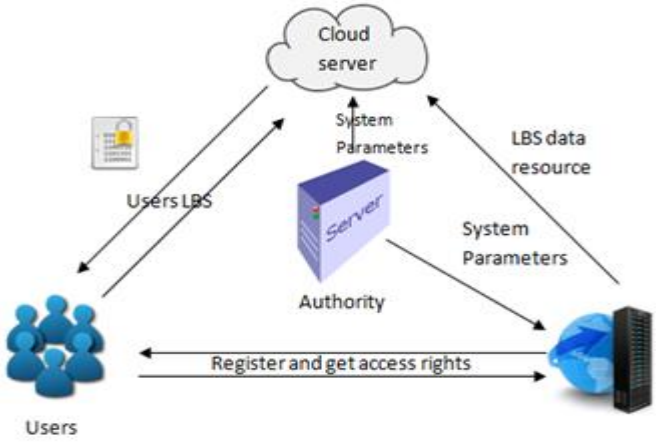


Fig.1. System Architecture.

- AU is an organization which initializes the whole system by generating and sending system parameters to LP and CS respectively.
- LP (i.e., the LBS data owner) owns abundant and accurate LBS data, and can provide polygons spatial query to the registered users. With the advancement in cloud computing, LP tends to outsource his/her LBS data to CS. Therefore, LP mainly performs two functions: outsourcing LBS data to CS and providing LU's registration system. In order to guarantee the confidentiality of LBS data, LP will perform some encryption operations before outsourcing LBS data to CS. With LU's registration system, LP can grant LU the right of sending polygons spatial query, and then the registered LU can be authenticated in CS.
- CS (i.e., the encrypted data storage and process server) stores abundant encrypted LBS data items from LP, and provides polygons spatial query services for the registered LU. CS mainly performs two functions: authenticating LU and processing polygons spatial searching over encrypted data. After receiving the query information from LU, CS first uses authentication technique to check LU's identity, and then processes the polygons spatial query in ciphertext with LU's encrypted query. Although CS is featured with high performance in computation and storage, since thousands of LU will query the LBS data at the same time, the efficiency of computation and communication in CS are still challenging.
- LU is the registered user of LP, and can query the outsourced LBS data items in CS. In order to provide

LU more convenient LBS range query, the system supports LU to define the search area (i.e., any convex) independently. In addition, LU will perform some encryption operations during the process of polygons spatial query to guarantee the privacy of query information. Moreover, in order to lower energy costs, the encryption efficiency of mobile devices is also very prerequisite.

B. System Implementation

In this section, we present our Polaris, which mainly consists of three phases: system initialization, cloud server data creation, privacy-preserving location based services. The conceptual architecture of Polaris can be depicted in Fig.2. After AU sends system parameters to CS and LP, LP outsources the index and encrypted LBS items to CS, and provides registration for LU in cloud server data creation. Then, LU can request for LBS through encrypted query information, and CS executes the special polygons spatial query algorithm to search the required LBS data items by traversing all encrypted LBS data items and send back the encrypted result to LU in privacy-preserving location based services.

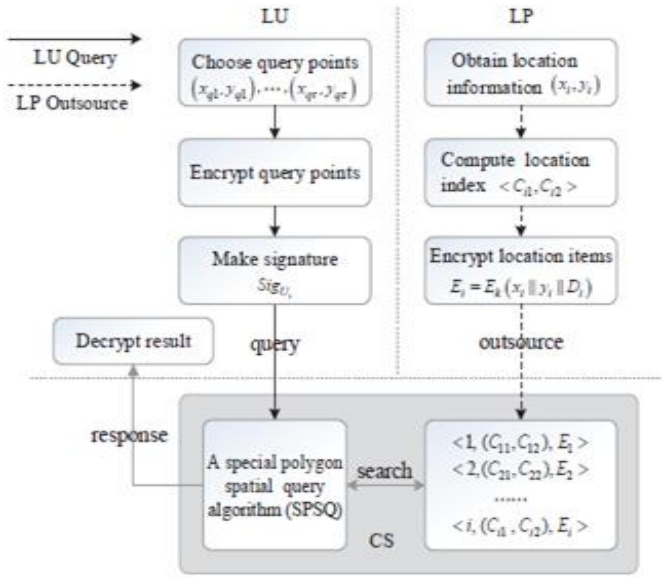


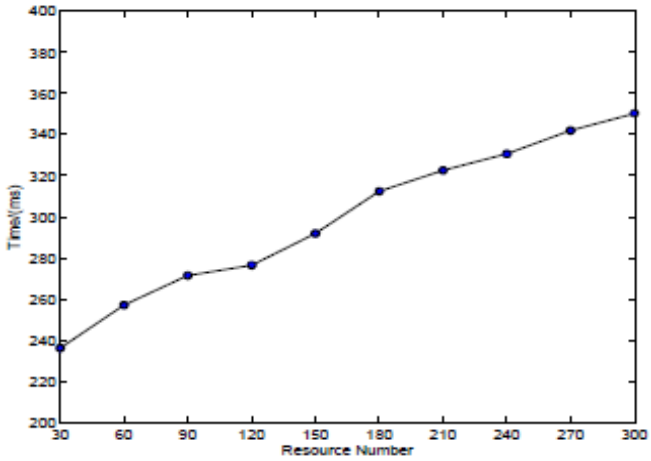
Fig.2. The Conceptual architecture of Polaris.

IV. SIMULATION AND ANALYSIS

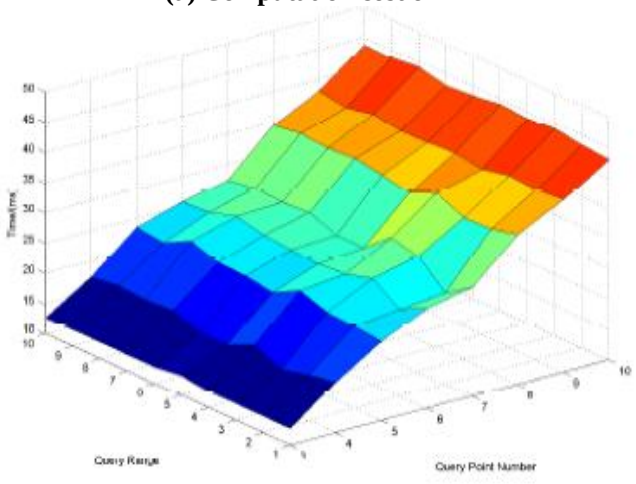
LP: In our proposed Polaris, LP outsources his/her LBS data to CS. Before being sent to CS, each LBS data item should be encrypted to (C_{i1},C_{i2}) as shown in IV-B. The factorimpacting the computation overhead of LP is the number ofspatial resources. Therefore, different number of resources arechosen to illustrate the computation overhead of LP. As shownin Fig. 3(a), the numbers of resources are selected from 30to 300. It is obvious that the computation overhead of LP increases linearly as the number of resources increase. The reason is that when LP outsources his/her LBS dataset to CS, each LBS data should be operated to obtain C_{i1},C_{i2} and E_k,which will lead to the linear increase of computation overhead with the increase of resources' number.

LU: The query response time of LU is an important factor illustrating our proposed Polaris framework. Therefore, different numbers of query points and query ranges are chosen to illustrate the computation cost of LU. Specifically, we set the resource number is 100, query points are chosen from 3 to 10, and the query ranges are set from 1to 10 times more than basic range. As shown in Fig. 3(b), with the increase of query points' number, LU's overhead increases linearly and the query range has no impact on LU. It is obvious that the total computation overhead in LU is less than 200milliseconds, and only once communication.

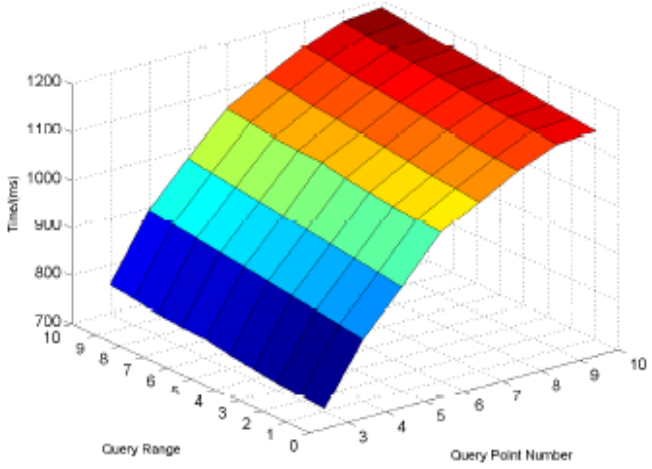
CS: In our proposed Polaris framework, after receiving a query request from LU, CS will compute the search criteria Tsi for each LU's query point using bilinear pairing over composite order group for each resource in query region, which is the mainly computation overhead of CS. We assume that the factors impacting the computation overhead of CS are the number of query points and LU's query range. Specifically, query points are chosen from 3 to 10, and the query range are set from 1 to 10 times more than basic range in Fig. 3(c). It is obvious that the computation overhead increases linearly with the increase of query points' number and query range. From the above analysis, the proposed Polaris framework is indeed efficient in terms of computation and communication cost, which is suitable for the smart phone and cloud server.



(a) Computation cost of LP



(b) Computation cost of LU



(c) Computation cost of CS

Fig.3. Computation complexity of LP, LU and CS.

V. CONCLUSION

In this paper, we have proposed an efficient and privacy-preserving polygons spatial query framework for location-based services, named Polaris. Based on an improved efficient homomorphic encryption technology over composite order group, the proposed Polaris can achieve query polygons privacy preservation and confidentiality of LBS data. Specifically, for an LBS query request from a registered LU, the LBS query execution is directly performed over ciphertext on CS without decryption, and the result of LBS query can only be decrypted by LU. Thus, LU can get accurate LBS query result without divulging his/her query information.

VI. REFERENCES

[1] Hui Zhu,Fen Liu, and Hui Li,"Efficient and Privacy-preserving Polygons SpatialQuery Framework for Location-based Services", IEEE INTERNET OF THINGS JOURNAL, Volume:4 , Issue: 2 , April 2017, pp. 536 - 545..

[2] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey ofmobile 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, "Enablingfine-grained multi-keyword search supporting classified sub-dictionariesover encrypted cloud data," 2015.

[4] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchableencryption of mobile cloud networks: when qoe meets qop," WirelessCommunications, IEEE, vol. 22, no. 4, pp. 74–80, 2015.

[5] H. Zhu, T. Liu, G. Wei, and H. Li, "Ppas: privacy protection authenticationscheme 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 adaptivekey evolution in smart grid," Parallel and Distributed Systems, IEEETransactions on, vol. 25, no. 8, pp. 2053–2064, 2014.

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

[8] L. Li, R. Lu, and C. Huang, "Eplq: Efficient privacy preservinglocation-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.

Author's Profile:

Mangalagiri Narmadha has received herB.Tech degree in Computer Science and Engineering from Dhanalaksh-mi Srinivas an College of Engineering And Technology affiliated to Anna University, Tamil Nadu in 2011. Pursuing M.Tech degree from Gokula Krishna College of Engineering, affiliated to JNTU, Anantapur.

R.M.Mallika has received her B.Tech Degree in Computer Science and Engineering and M.Tech degree in Information Technology from JNTU, Hyderabad in 2001 and Satyabhama University, in 2009 respectively. She is dedicated to teaching field from the last 13 years. She has guided 8 P.G and 50 U.G students. Her research area included Soft Computing. At present she is working as Associate Professor in Gokula Krishna College of Engineering, Sullurpeta, Nellore, Andhra Pradesh, India.