ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/8578
DOI URL: http://dx.doi.org/10.21474/IJAR01/8578

RESEARCH ARTICLE

SPATIAL LOCATION OF ASSURANCE WITH WITNESS OF MUTUAL PROOFS PROVIDING PRIVACY FOR MOBILE USERS.

Gadipalli Bhavani[1] and Vishwesh Nagamalla[2].

1. M.Tech Student, Dept of CSE, Sreenidhi Institute Of Science And Technology, Ts.
2. AsstProfessor, Dept of CSE, Sreenidhi Institute Of Science And Technology, Ts.

Manuscript Info

Manuscript History
Received: 14 December 2018
Final Accepted: 16 January 2019
Published: February 2019

Key words:-
Location-based services (LBS), outsourced encrypted data, privacy-enhancing technology, spatial range query.

Abstract

In our safe tourist application or travelling we aims to outsource the lbs data from the lbs provider to the cloud and from the cloud to the lbs provider which protects the privacy related issues of the lbs data. Initially lbs user query for a place to the lbs provider, lbs provider in turn upload the details to the cloud but in the form of encrypted text to prevent the cloud from stealing the data. Lbs users in turn decrypt the details by the personal password send by the lbs provider to the lbs user. When the query of the lbs user matches the details in the cloud the lbs user will retrieve the details and make use of it. In this application it is shown with the demo of a tourist requesting for tourist places tourist is the lbs user and admin is the lbs provider .With the pervasiveness of smart phones, location based services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user’s location privacy. In this paper, aiming at spatial range query, popular LBS providing information About POIs (Points of Interest), we present an efficient and privacy-preserving location based query solution, called SPATIAL RANGE. To reduce query latency, we further design a privacy-preserving tree index structure in SPATIAL RANGE. Detailed security analysis confirms the security properties of SPATIAL RANGE. In addition, extensive experiments are conducted, and the results demonstrate that spatial range is very efficient in privacy preserving spatial range query over outsourced encrypted data. In particular, for a mobile LBS user using an Android phone, around 0.9 second is needed to generate a query; and it also only requires a commodity workstation, which plays the role of the cloud in our experiments, a few seconds to search POIs.

Introduction:-

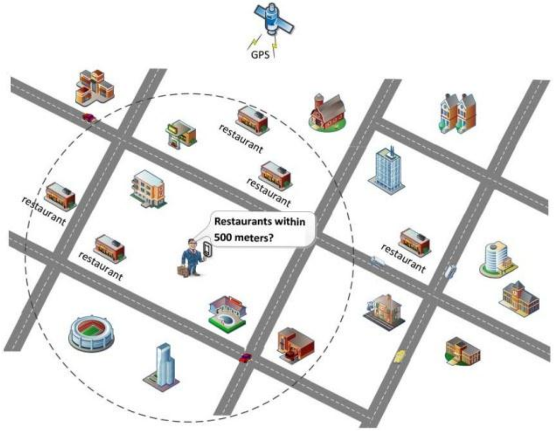
A FEW decades ago, location-based services (LBS) wereused in military only. Today, thanks to advances in information and communication technologies, more kinds of LBShave appeared, and they are very useful for not only organiza-tions but also individuals. Let us take the spatial range query,one kind of LBS that we will focus in this paper, as an exam-ple. Spatial range query is a widely used LBS, which allows auser to find points of interest (POIs) within a given distance tohis/her location, i.e., the query point. As illustrated in Fig. 1,with this kind of LBS, a user

Corresponding Author:-GadipalliBhavani.
Address:-M.Tech Student, Dept of CSE, Sreenidhi Institute Of Science And Technology, Ts.

could obtain the records of allrestaurants within walking distance (say 500 m). Then, theuser can go through these records to find a desirable restaurant
considering price and reviews.

While LBS are popular and vital, most of these services today including spatial range query require users to submit their locations, which raises serious concerns about the leak- ing and misusing of user location data. For example, criminals may utilize the data to track potential victims and predicttheir locations.Foranotherexample,somesensitivelocationdataoforganizationusersmayinvolvetradesecretornationalsecurity. ProtectingtheprivacyofuserlocationinLBShasattractedcon- siderable interest. However, significant challenges still remain in the design of privacy-preserving LBS, and new challenges ariseparticularlyduetodataoutsourcing.Inrecentyears,there is a growing trend of outsourcing data including LBS data because of its financial and operational benefits. Lying at the intersectionofmobilecomputingandcloudcomputing,design- ingprivacy-preservingoutsourcedspatialrangequeryfacesthechallengesbelow.

Fig. 1:-Example of spatial range query.



Challenge on querying encrypted LBS data. The LBS provider is not willing to disclose its valuable LBS data to the cloud. As illustrated in Fig. 2, the LBS provider encrypts and outsources private LBS data to the cloud, and LBS users query the encrypted data in the cloud. As a result, querying encrypted LBS data without privacy breachisabigchallenge,andweneedtoprotectnotonly the user locations from the LBS provider and cloud but also LBS data from thecloud.

Challengeontheresourceconsumptioninmobiledevices. Many LBS users are mobile users, and their terminals are smart phones with very limited resources. However, the cryptographic or privacy-enhancing techniques used to realize privacy-preserving query usually result in high computational cost and/or storage cost at userside.

Challenge on the efficiency of POI searching. Spatial rangequeryisanonlineservice,andLBSusersaresensi- tiveto query latency. To provide good user experiences, thePOIsearchperformingatthecloudsidemustbeFig. 2.System model of outsourced LBS under consideration.

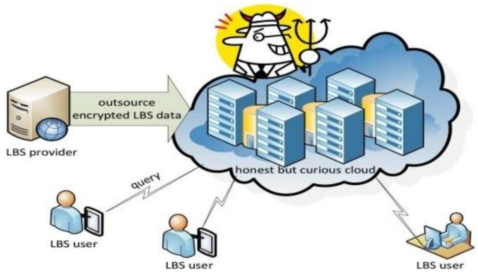


Fig. 2:-System model of outsourced LBS under consideration.

vectors is in a given range. The two vectors contain the location information of the POI and the query, respec- tively. Based on this discovery and our IPRE scheme, spatial range query without leaking location informa- tion can be achieved. To avoid scanning all POIs to find matchedPOIs,wefurtherexploitanovelindexstructure named sˆs-tree, which conceals sensitivelocation done in a short time (e.g., a few seconds at most). Again, the techniques used to realize privacy-preserving query usually increase the search latency.

Challenge on security. LBS data are about POIs in real world. It is reasonable to assume that the attacker may havesomeknowledgeaboutoriginalLBSdata.Withsuch knowledge, known-sample attacks are possible (elabo- rated later in SectionII).

Recently, there are already some solutions for privacy- preserving spatial range query [1]–[6]. However, as elaborated in Section VIII later, existing solutions cannot address all the above challenges. Aiming at these, in this paper, we propose an efficient solution for privacy-preserving spatial range query named SPATIAL RANGE, which allows queries over encrypted LBS data without disclosing user locations to the cloud or LBS provider. To protect the privacy of user location in SPATIAL RANGE, we design a novel predicate-only encryption scheme for inner product range (IPRE scheme for short), which, to the best of our knowledge, is the first predicate/predicate-only scheme of this kind. To improve the performance, we also design a privacy- preservingindexstructurenamedsˆs-tree.Specifically,themain contributions of this paper are threefolds.

WeproposeIPRE,whichallowstestingwhethertheinner product of two vectors is within a given range without disclosing the vectors. In predicate encryption, the key corresponding to a predicate f can decrypt a ciphertext if and only if the attribute of the ciphertextx satisfies the predicate, i.e., f (x) = 1. Predicate-only encryption is a special type of predicate encryption not designed for encrypting/decrypting messages. Instead, it reveals that whether f (x) = 1 or not. Predicate-only encryption schemes supporting different types of predicates [7], [8] have been proposed for privacy-preserving query on out- sourceddata.Tothebestofourknowledge,theredoesnot exist predicate/predicate-only scheme supporting inner product range. Though our scheme is used for privacy- preserving spatial range query in this paper, it may be applied in other applications aswell.

We propose SPATIAL RANGE, an efficient solution for privacy-preservingspatialrangequery.Inparticular,weshowthat whether a POI matches a spatial range query or not can be tested by examining whether the inner

Related Work:-

Location Verification using Secure Distance Bounding Protocols AUTHORS: D. Singelee and B. Preneel.authentication in conventional networks (Internet) is usually based upon (e.g password), something you have (e.g smartcard)(biometrics). In mobile ad–hoc networks, location information can also be used to authenticate devices and users. We will focus on how a prover can securely show that he is within a certain distance to a verifier. They proposed the distance bounding protocol as a secure solution.

Enhanced Architecture for Privacy Preserving Data Integration in a Medical Research EnviornmentAUTHORS: FarhanaJabeen, Zara Hamid. Recent advancement in digital and communication technologies has brought privacy aspects to the forefront.Designing robust privacy preserving policies to strengthen the trust of patients in Electroinc Health Records(EHRs) is imperative for its wide spread acceptance and success.

Light weight Location Verification Algorithm For Wireless Sensor NetworksAUTHORS: YawenWei and Yong Guan. The knowledge of sensors’ locations is crucial information for many applications in Wireless Sensor Networks (WSNs). When sensor nodes are deployed in hostile environments, the localization schemes are vulnerable to various attacks. Experiment results show that our on-spot and in-region algorithms can verify sensors’ locations with high detection rate and low false positive rate.

Stamp:-

Enabling Privacy-Preserving Location Proofs for Mobile Users AUTHORS:XinleiWang ; AmitPande ; Jindan Zhu ; PrasantMohapatra STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted

Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach.

Design Goal:-

In this section, we formalize the system model and attack models considered in this paper, and identify the design goal.

SystemModel:-

Privacy-preserving POI query has been studied in two set- tings of LBS: 1) public LBS and 2) outsourced LBS. In this paper,wefocusonthelattersetting.Intheformersetting,there is an LBS provider holding a spatial database of POI records in plaintext, and LBS users query POIs at the provider's site. In outsourced LBS, as shown in Fig. 2, the system consists of three kinds of entities, LBS provider, LBS users, and cloud, as follows.

The LBS provider has abundant of LBS data, which are POI records. The LBS provider allows authorized users (i.e.,LBSusers)toutilizeitsdatathroughlocation-based queries.Becauseofthefinancialandoperationalbenefitsofdataoutsourcing,theLBSprovideroffersthequery

services via the cloud. However, the LBS provider is not willing to disclose the valuable LBS data to the cloud. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted data to the cloud.

The cloud has rich storage and computing resources. It storestheencryptedLBSdatafromtheLBSprovider,and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBSusers.

LBS users have the information of their own locations, and query the encrypted records of nearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

AttackModels:-

Similar to most previous works on outsourced data query, the cloud is assumed honest but curious and considered as the potentialattackerinthiswork.Thatis,thecloudwouldhonestly store and search data as requested; however, the cloud would also have financial incentives to learn those stored LBS data and user location data in query. Because both LBS data and user location data are valuable, they should be protected and hidden from the cloud. In general, in the outsourced LBS set- ting, the cloud can observe both queries from LBS users and encryptedLBSdatafromtheLBSprovider,whichcouldbeanadvantagetolearnuserlocations.Therefore,assumingdifferent abilities of the attacker, there are mainly four attack models in outsourced LBSsetting.

Ciphertext-only attack. In this model, the attacker is able to observe the ciphertexts of POIs' locations and queries but does not know the plaintexts. Obviously, every cloud has this ability. This is a weak attackmodel.

Known-sample attack. In this model, the attacker knows theplaintextsofsomePOIs'locationsand/orqueries.The attacker also knows that their corresponding ciphertexts must exist in all the ciphertexts observed by the attacker. However, the attacker does not know which ciphertext is correspondingtoaknownplaintext.Utilizingsuchinformation, the attacker may be able to reveal the plaintext corresponded to any given ciphertext. Such information is not hard to obtain if the attacker has the background knowledge that the LBS database must contain the POIs of certain type in a certainarea.

Known-plaintextattack.Inthismodel,theattackerknows the plaintexts of some POIs' locations and/or queries as well as their corresponding ciphertexts. Utilizing this information, the attacker may be able to reveal the plain- texts corresponded to otherciphertexts.

Access-pattern attack. In this model, the attacker has some background knowledge about the pattern of POI accessing. For example, the attacker knows that a known POI would be the most popular POI. If an encrypted POI appearsmostfrequentlyinqueryresults,itmustbethe

encrypted version of the known POI. Then, the attacker knows that corresponding query points must be close to the known POI.
Inadditiontotheaboveattacks,otherattackssuchasinsider attacks may be possible. In this paper, we consider ciphertext- onlyandknown-sampleattacks,whichdonotrequireattackers with very strong abilities. We will leave the attacks requiring very strong abilities for futurestudy.

Design Goal:-
Under the outsourced LBS system model, our design goal is to develop an efficient, accurate, and secure solution for privacy-preservingspatialrangequery.Specifically,thefollow- ing three objectives should beachieved.

Efficiency. As discussed in Section I, spatial range query has stringent performance requirements. A good solu- tion should not consume many resources of mobile LBS users,andthePOIsearchlatencyshouldbeacceptableforonlinequery.

Accuracy. It is desirable that a query result contains the exact records matching the query. False negatives would hurtuserexperience,whilefalsepositiveswouldincrease communication cost. Additional computational cost is alsorequiredattheusersidetofilteroutfalsepositives.

Security. The proposed solution should be resilient to ciphertext-only attacks and known-sample attacks. An accurateandefficientsolutionforspatialrangequery

already exists, which is resilient to ciphertext-only attacksbutnottoknown-sampleattacksandmorepower- fat tacks. The proposed solution should be more secure than the solution in[1].

Though subject to more powerful attacks such as known- plaintext attacks, the solution proposed in this paper still can be used in many situations where the attackers do not have the required abilities or knowledge. Our solution also has advan- tagesoverthesolutionsresilienttosuchattacks.Aswewillsee in the related works in Section VIII, such solutions are either very computationally costly or not applicable to outsourced LBS.

Ipre: a novel predicate-onlyencryption:-
Scheme for inner product range:-
In this section, we present IPRE, which will serve as the basisofourSPATIALRANGEsolutionforprivacy-preservingspatialrange query.

Overview:-
the proposed IPRE scheme allows computing inner products and comparing their values with a predefined range in a privacy-preserving way. As far as we know, our scheme is the firstpredicatepredicateonlyencryptionschemeforinnerproduct range. In IPRE, both attributes and predict are vector

IPRE scheme is a symmetric predicate-only encryption scheme, and it consists of four algorithms: 1) Setup algorithm for generating a public parameter PP, an attribute encryption key AK, and a predicate encryption key PK; Enc algorithm for encrypting attribute vectors to cipher texts; 3) GenToken algorithm for encrypting predicate vectors to tokens; and 4) Check algorithm for checking if a cipher text’s attribute

satisfies a token’s predicate:-
Setup Algorithm:-
The setup algorithm is a probabilistic algorithm, which takes a security parameter λ, the attribute/predicate vector length t,and an inner product range

Enc Algorithm:-
The algorithm of encrypting attribute vectors is a probabilistic algorithm, which takes an attribute vector Vj = (vj,1, vj,2, . . . , vj,t) and a random number sj∈ Fp as input

GenToken Algorithm:-
The token generation algorithm GenToken is a probabilistic algorithm, which takes a predicate vector Ui = (ui,1, ui,2, . . . , ui,t) and a random number hi ∈ Fp as input, and outputs Ki = (qi,1, qi,2, . . . , qi,n+1)

Check Algorithm:-

The check algorithm takes a ciphertextCj = (cj,1, cj,2, . . . , cj,n+1) of an attribute vector Vj and a token Ki = (qi,1, qi,2, . . . , qi,n+1) associated with a predicate vector

Results And Summary:-

In this paper, we propose an efficient solution for privacy-preserving spatial range query named SPATIAL RANGE, which allows queries over encrypted LBS data without disclosing user locations to the cloud or LBS provider.

To protect the privacy of user location in SPATIAL RANGE, we design a novel predicate-only encryption scheme for inner product range (IPRE scheme for short), which, to the best of our knowledge, is the first predicate/predicate-only scheme of this kind. To improve the performance, we also design a privacy preserving index structure named ˆss-tree. Specifically, the main contributions of this paper are three folds.

We propose IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. In predicate encryption, the key corresponding to a predicate f can decrypt a cipher text if and only if the attribute of the ciphertextx satisfies the predicate, i.e., f(x) = 1. Predicate-only encryption is a special type of predicate encryption not designed for encrypting/decrypting messages. Instead, it reveals that whether f(x) = 1 or not. Predicate-only encryption schemes supporting different types of predicates have been proposed for privacy-preserving query on outsourced data.

We propose SPATIAL RANGE, an efficient solution for privacy preserving spatial range query. In particular, we show that whether a POI matches a spatial range query or not can be tested by examining whether the inner product of two vectors is in a given range. The two vectors contain the location information of the POI and the query, respectively. Based on this discovery and our IPRE scheme, spatial range query without leaking location information can be achieved. To avoid scanning all POIs to find matched POIs, we further exploit a novel index structure named ˆss-tree, which conceals sensitive location information with our IPRE scheme.

Our techniques can be used for more kinds of privacypreserving queries over outsourced data. In the spatial range query discussed in this work, we consider Euclidean distance, which is widely used in spatial databases. Our IPRE scheme and ˆss-tree may be used for searching records within a given weighted Euclidean distance or great-circle distance as well.Weighted Euclidean distance is used to measure the dissimilarity in many kinds of data, while great-circle distance is the distance of two points on the surface of a sphere.

Advantages of proposed system:-

To the best of our knowledge, there does not existpredicate/predicate-only scheme supporting inner product range. Though our scheme is used for privacy preserving spatial range query in this paper, it may be applied in other applications as well.

Experiments on our implementation demonstrate that our solution is very efficient.Moreover, security analysis shows that Spatial Range is secure under known-sample attacks and cipher text-only attacks.
Using great-circle distance instead of Euclidean distance for long distances on the surface of earth is more accurate. By supporting these two kinds of distances, privacy-preserving similarity query and long spatial range query can also be realize

Results:-

In this result we created many user to providing privacy using IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. In predicate encryption, the key corresponding to a predicate f can decrypt a cipher text if and only if the attribute of the ciphertextx satisfies the predicate, i.e., f(x) = 1. Predicate-only encryption is a special type of predicate encryption not designed for encrypting/decrypting messages. Instead, it reveals that whether f(x) = 1 or not. Predicate-only encryption schemes supporting different types of predicates have been proposed for privacy-preserving query on outsourced data.

Conclusion:-

In this paper, we have proposed SPATIAL RANGE, an efficient privacy-preservingspatialrangequerysolutionforsmartphones,which preserves the privacy of user location, and achieves confiden- tiality of LBS data. To realize SPATIAL RANGE, we have designed an IPRE and a novel privacy-preserving index tree named sˆs-tree. SPATIAL RANGE's efficacy has been evaluated with theoretical analy- sis and experiments, and detailed analysis shows its security againstknown-sampleattacksandciphertext-onlyattacks.Our techniques have potential usages in other kinds of privacy- preserving queries. If the query can be performed through comparing inner products to a given range, the proposed IPRE and sˆs-treemay be applied to realize privacy-preserving query. Two potential usages are privacy-preserving similar- ity query and long spatial range query. In the future, we will design solutions for these scenarios and identify more usages.

References:-

1. Gutscher, "Coordinate transformation—A solution for the privacy problem of location based services?" in Proc. 20th Int. Parallel Distrib. Process. Symp. (IPDPS'06), Rhodes Island, Greece, Apr. 25–29, 2006, p.424.
2. W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in Proc. SIGMOD, 2009, pp.139–152.
3. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not neces- sary," in Proc. SIGMOD, 2008, pp.121–132.
4. X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in Proc. 30th Int. Conf. Data Eng. (ICDE), 2014, pp.640–651.
5. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private informa- tionretrieval," J. ACM, vol. 45, no. 6, pp. 965–981,1998.
6. F. Olumofin and I. Goldberg, "Revisiting the computational practicality of private information retrieval," in Financial Cryptography and Data Security. New York, NY: Springer, 2012, pp.158–172.
7. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting dis- junctions, polynomial equations, and inner products," in Proc. 27th Ann. Int. Conf. Theory Appl. Cryptograph. Tech. Adv. Cryptol. (EUROCRYPT '08), Istanbul, Turkey, Apr. 13–17, 2008, pp.146–162.
8. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. 4th Theory Cryptograph. Conf. (TCC'07), Amsterdam, The Netherlands, Feb. 21–24, 2007, pp.535–554.
9. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615,2003.
10. A. White and R. Jain, "Similarity indexing with the ss-tree," in Proc. 12th Int. Conf. Data Eng. (ICDE), 1996, pp.516–523.
11. Guttman, "R-trees: A dynamic index structure for spatial searching," in Proc. Annu. Meeting (SIGMOD'84), Boston, MA, USA, Jun. 18–21, 1984, pp.47–57.
12. T. K. Dang, J. Küng, and R. Wagner, "The sh-tree: A super hybrid index structure for multidimensional data," in Proc. 12th Int. Conf. Database Expert Syst. Appl. (DEXA' 01), Munich, Germany, Sep. 3–5, 2001, pp.340–349.
13. B.-Y. Yang and J.-M. Chen, "All in the XL family: Theory andpractice," in Proc. Int. Conf. Inf. Secur. Cryptol, 2004, pp.67–86.
14. G.Ars,J.-C.Faugere,H.Imai,M.Kawazoe,andM.Sugita,"Comparison betweenXLandGröbnerbasisalgorithms,"inProc.ASIACRYPT,2004, pp.338–353.
15. B. Yao, F. Li, and X. Xiao, "Secure nearest neighbor revisited," in Proc. IEEE 29th Int. Conf. Data Eng. (ICDE'13), 2013, pp.733–744.
16. Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neigh-borqueryoverencrypteddatainoutsourcedenvironments,"inProc.IEEE 30th Int. Conf. Data Eng. (ICDE), 2014, pp.664–675.
17. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neigh- bor queries using space transformation to preserve location privacy," in Advances in Spatial and Temporal Databases. New York, NY, USA: Springer, 2007, pp.239–257.
18. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidi- mensional range queries over outsourced data," VLDB J., vol. 21, no. 3, pp. 333–358,2012.
19. I.-T.Lien,Y.-H.Lin,J.-R.Shieh,andJ.-L.Wu,"Anovelprivacypreserv- ing location-based service protocol with secret circular shift for k-NN search," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 6, pp. 863–873, Jun.2013.
20. M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," VLDB J., vol. 19, no. 3, pp. 363–384,2010.
21. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig, "Multi- dimensional range query over encrypted data," in Proc. IEEE Symp. Secur. & Privacy, 2007, pp.350–364.

22. B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: Scalable multi- dimensional range search over encrypted cloud data withtree-based index," in Proc. 9th ACM Symp. Inf. Comput. Commun. Secur.,2014, pp.111–122.
23. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. SIGMOD, 2004, pp.563–574.
24. J. Shao, R. Lu, and X. Lin, "Fine: A fine-grained privacy-preserving location-based service framework for mobile devices," in Proc. IEEE INFOCOM, 2014, pp.244–252.
25. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Proc. eurocrypt, 2009, pp.224–241.
26. P. Wang and C. Ravishankar, "Secure and efficient range queries on out- sourceddatabasesusingRp-trees,"inProc.Int.Conf.DataEng.(ICDE), 2013, pp.314–325.
27. R. Beresford and F. Stajano, "Location privacy in pervasive comput- ing," Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan./Mar.2003.
28. Y. Zhu, D. Ma, D. Huang, and C. Hu, "Enabling secure location-based services in mobile cloud computing," in Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput., 2013, pp.27–32.
29. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication techniqueusingdummiesforlocation-basedservices,"inProc.Int.Conf. Perv. Serv. (ICPS), 2005, pp.88–97.
30. C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati, "Location privacy protection throughobfuscation-based techniques," in Proc. Data Appl. Secur. XXI, 2007, pp.47–60.
31. M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. 1st Int. Conf. Mobile Syst. Appl. Serv., 2003, pp.31–42.
32. M. F. Mokbel, C.-Y.Chow, and W. G. Aref, "The new Casper: Query processingforlocationserviceswithoutcompromisingprivacy,"inProc. 32nd Int. Conf. Very Large Data Bases (VLDB'06), 2006, pp.763–774.