A New Mechanism for Encrypted Data with Efficient Privacy-Preserving Location-Based Query: EPLQ

Kola Satish Kumar[1], Anuradha Tutika[2], Appala Raju Samanthula[3]

[1]M.Tech (CSE), Raghu Engineering College, Dakamarri, Visakhapatnam, A.P., India.
[2-3]Assistant professor, Dept of Cse, Raghu Engineering College, Dakamarri, Visakhapatnam, A.P., India.

Abstract *— location-based services (LBS) were used in military only. Today, thanks to advance in communication technologies and information technologies, more kinds of location based services have appeared, and they are useful for not only organizations but also individuals. Mobile LBS are services enhanced with positional data, which are provided by mobile apps using GPS, Dmaps, and other techniques. Many mobile apps provide interesting and convenient lbs and functions. The mobile app Yelp recommends nearby shops, restaurants, etc. In the social network mobile app Loopt, the users receive notifications Whenever their friends are nearby. The mobile app Waze reports nearby traffic jams, gas stations and friends. Users can access these services via the desktop, mobile phone, Personal Digital Assistant pager, Web browser , or other devices. Diverse applications include fleet tracking, emergency dispatch, roadside assistance, navigation, and more. The aim of safe tourister application to outsource the location based service (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 have received considerable attention and become more popular and vital recently. However, the use of LBS also has a potential threat to user's location privacy. In this paper, aiming at spatial range query, popular LBS providing information About Points of Interest, we present an effective and privacy-preserving LBS solution, called EPLQ. To reduce query latency, we further design a privacy-preserving tree index structure in EPLQ. Detailed security analysis confirms the security properties of EPLQ.*

Keywords *—* **Location privacy, security, location-based social applications, Location-based services (LBS), spatial range query, outsourced encrypted data, Effective and Privacy Preserving Location-Based query (EPLQ)..**

1. INTRODUCTION

Smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. Within these markets, a new wave of geo-social applications is fully exploiting GPS location services to provide a "social" interface to the physical world. Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geo-

social applications operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain, physical stalking, and to gather legal evidence. Even more disturbing, it seems that less than a week after Facebook turned on their popular "Places" feature for tracking users' locations, such location data was already used by thieves to plan home invasions . Clearly, mobile social networks of tomorrow require stronger privacy properties than
the opento- all policies available today.

Existing systems have mainly taken three approaches to improving user privacy in geo-social systems: (a) introducing uncertainty or error into location data relying on trusted servers or intermediaries to apply anonymization to user identities and private data , and (b) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices, and even on the servers in answering queries such as nearest-neighbor and range queries.

The challenge, then, is to design mechanisms that efficiently protect user privacy without sacrificing the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers. More specifically, we target geo-social applications, and assume that servers (and any intermediaries) can be compromised and, therefore, are untrusted. To limit misuse, our goal is to limit accessibility of location information from global visibility to a user's social circle. We identify two main types of queries necessary to support the functionality of these geo-social applications: point queries and nearest-neighbor (*kNN*) queries. Point queries query for location data at a particular point, whereas *kNN* queries query for k nearest data around a given location coordinate (or up to a certain radius). Our goal is to support both query types in an efficient fashion, suitable for today's mobile devices.To address this challenge, in this paper, we propose LocX (short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here onwards). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data. Thus, we can partition location data based on users' social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real world locations without a secret, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on LocX lightweight and suitable for running on today's mobile devices.

2. LITERATURE SURVEY

1) Coordinate transformation—A solution for the privacy problem of location based services?

AUTHORS: A. Gutscher

Protecting location information of mobile users in location based services (LBS) is a very important but quite difficult and still largely unsolved problem. Location information has to be protected against unauthorized access not only from users but also from service providers storing and processing the location data, without restricting the functionality of the system. This paper discusses why existing privacy enhancing techniques are insufficient to solve this problem and proposes a new approach basing on coordinate transformations. It shows how location information can be rendered illegible in such a way that it is still possible to perform processing operations required by LBS

2) Secure kNN computation on encrypted databases

AUTHORS: W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis

Service providers like Google and Amazon are moving into the SaaS (Software as a Service) business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruit businesses to run applications on their platforms. To enforce security and privacy on such a service model, we need to protect the data running on the platform. Unfortunately, traditional encryption methods that aim at providing "unbreakable" protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. In this paper we discuss the general problem of secure computation on an encrypted database and propose a SCONEDB Secure Computation ON an Encrypted DataBase) model, which captures the execution and security requirements. As a case study, we focus on the problem of k-nearest neighbor (kNN) computation on an encrypted database. We develop a new asymmetric scalar-product-preserving encryption (ASPE) that preserves a special type of scalar product. We use APSE to construct two secure schemes that support kNN computation on encrypted data; each of these schemes is shown to resist practical attacks of a different background knowledge level, at a different overhead cost. Extensive performance studies are carried out to evaluate the overhead and the efficiency of the schemes.

3) Private queries in location based services: Anonymizers are not necessary

AUTHORS: G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. T

Mobile devices equipped with positioning capabilities (e.g., GPS) can ask location-dependent queries to Location Based Services (*LBS*). To protect privacy, the user location must not be disclosed. Existing solutions utilize a trusted anonymizer between the users and the LBS. This approach has several drawbacks: (*i*) All users must trust the third party anonymizer, which is a single point of attack. (*ii*) A large number of cooperating, trustworthy users is needed. (*iii*) Privacy is guaranteed only for a single snapshot of user locations; users are not protected against correlation attacks (e.g., history of user movement).

We propose a novel framework to support private location-dependent queries, based on the theoretical work on Private Information Retrieval (*PIR*). Our framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared to existing work, our approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. We use our framework to implement approximate and exact algorithms for nearest-neighbor search. We optimize query execution by employing data mining techniques, which identify redundant computations. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice.

4) Practical *k* nearest neighbor queries with location privacy

AUTHORS: X. Yi, R. Paulet, E. Bertino, and V. Varadharajan

In mobile communication, spatial queries pose a serious threat to user location privacy because the location of a query may reveal sensitive information about the mobile user. In this paper, we study k nearest neighbor (kNN) queries where the mobile user queries the location-based service (LBS) provider about k nearest points of interest (POIs) on the basis of his current location. We propose a solution for the mobile user to preserve his location privacy in kNN queries. The proposed solution is built on the Paillier public-key cryptosystem and can provide both location privacy and data privacy. In particular, our solution allows the mobile user to retrieve one type of POIs, for example, k nearest car parks, without revealing to the LBS provider what type of points is retrieved. For a cloaking region with n×n cells and m types of points, the total communication complexity for the mobile user to retrieve a type of k nearest POIs is O(n+m) while the computation complexities of the mobile user and the LBS provider are O(n + m) and O(n^2m), respectively. Compared with existing solutions for kNN queries with location privacy, our solutions are more efficient. Experiments have shown that our solutions are practical for kNN queries.

5) Revisiting the computational practicality of private information retrieval

AUTHORS: F. Olumofin and I. Goldberg

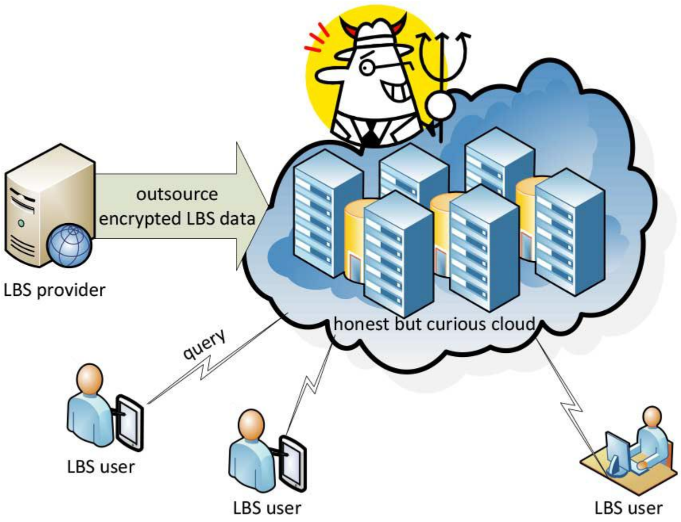
Remote servers need search terms from the user to complete retrieval requests. However, keeping the search terms private or confidential without undermining the server's ability to retrieve the desired information is a problem that private information retrieval (PIR) schemes are designed to address. A study of the computational practicality of PIR by Sion and Carbunar in 2007 concluded that no existing construction is as efficient as the trivial PIR scheme -- the server transferring its entire database to the client. While often cited as evidence that PIR is impractical, that paper did not examine multi-server information-theoretic PIR schemes or recent single-server lattice-based PIR schemes. In this paper, we report on a performance analysis of a single-server lattice-based scheme by Aguilar-Melchor and Gaborit, as well as two multi-server information-theoretic PIR schemes by Chor et al. and by Goldberg. Using analytical and experimental techniques, we find the end-to-end response times of these schemes to be one to three orders of magnitude (10---1000 times) smaller than the trivial scheme for realistic computation power and network bandwidth. Our results extend and clarify the conclusions of Sion and Carbunar for multi-server PIR schemes and single-server PIR schemes that do not rely heavily on number theory.

3. RELATED WORK

Prior work on privacy in general location-based services (LBS). There are mainly three categories of proposals on providing location privacy in general LBSs that do not specifically target social applications. First is spatial and temporal cloaking , wherein approximate location and time is sent to the server instead of the exact values. The intuition here is that this prevents accurate identification of the locations of the users, or hides the user among k other users (called k-anonymity and thus improves privacy. This approach, however, hurts the accuracy and timeliness of the responses from the server, and most importantly, there are several simple attacks on these mechanisms that can still break user privacy. Pseudonyms and silent times [14] are other mechanisms to achieve cloaking, where in device identifiers are changed frequently, and data is not transmitted for long periods at regular intervals. This, however, severely hurts functionality and disconnects users. The key difference between these approaches and our work is that they rely on trusted intermediaries, or trusted servers, and reveal approximate real world location to the servers in plain-text. In LocX, we do not trust any intermediaries or servers. On the positive side, these approaches are more general and, hence, can apply to many location-based services, while LocX focuses mainly on the emerging geo-social applications.

The second category is location transformation, which uses transformed location coordinates to preserve user location privacy. One subtle issue in processing nearest-neighbor queries with this approach is to accurately find all the real neighbors. Blind evaluation using Hilbert Curves, unfortunately, can only find approximate neighbors. In order to find real neighbors, previous work either keeps the proximity of transformed locations to actual locations and incrementally processes nearest-neighbor queries, or requires trusted third parties to perform location transformation between clients and LBSA servers. In contrast, LocX does not trust any third party and the transformed locations are not related to actual locations. However, our system is still able to determine the actual neighbors, and is resistant against attacks based on monitoring continuous queries.

The third category of work relies on Private Information Retrieval (PIR) to provide strong location privacy. Its performance, although improved by using special hardware, is still much worse than all the other approaches, thus it is unclear at present if this approach can be applied in real LBSs.



4. CONCLUSION

In this paper, we have proposed EPLQ, an efficient privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. To realize EPLQ, we have designed an IPRE and a novel privacy-preserving index tree named ˆ *ss*-tree. EPLQ’s efficacy has been evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and ciphertext-only attacks. 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 ˆ *ss*-tree may be applied to realize privacy-preserving query. Two potential usages are privacy-preserving similarity query and long spatial range query. In the future, we will design solutions for these scenarios and identify more usages.

REFERENCES

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, “Peoplenet: engineering a wireless virtual social network,” in Proc. of MobiCom, 2005.

[2] M. Hendrickson, “The state of location-based social networking,” 2008.

[3] P. Mohan, V. N. Padmanabhan, and R. Ramjee, “Nericell: rich monitoring of road and traffic conditions using mobile smartphones,” in Proc. of SenSys, 2008.

[4] G. Ananthanarayanan, V. N. Padmanabhan, L. Ravindranath, and C. A. Thekkath, “Combine: leveraging the power of wireless peers through collaborative downloading,” in Proc. of MobiSys, 2007.

[5] M. Siegler, “Foodspotting is a location-based game that will make your mouth water,” http://techcrunch.com/2010/03/04/foodspotting/.

[6] http://www.scvngr.com.

[7] B. Schilit, J. Hong, and M. Gruteser, “Wireless location privacy protection,” Computer, vol. 36, no. 12, pp. 135–137, 2003.

[8] F. Grace, “Stalker Victims Should Check For GPS,” Feb. 2003, www.cbsnews.com.

[9] DailyNews, “How cell phone helped cops nail key murder suspect secret ’pings’ that gave bouncer away,” Mar. 2006.

[10] “Police: Thieves robbed homes based on facebook, social media sites,” WMUR News, September 2010, http://www.wmur.com/r/24943582/detail.html.

[11] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. of Mobisys, 2003.

[12] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: A privacyaware location-based database server,” in ICDE, 2007.

[13] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in Proc. of ICDCS, 2005.

[14] T. Jiang, H. J. Wang, and Y.-C. Hu, “Preserving location privacy in
wireless lans,” in Proc. of MobiSys, 2007.

[15] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” TKDE, 2007.

[16] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in *Proc. IEEE 30th Int. Conf. Data Eng. (ICDE)*, 2014, pp. 664–675.

[17] A. Khoshgozaran and C. Shahabi, “Blind evaluation of nearest neighbor 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] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, “Secure multidimensional 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, and J.-L.Wu, “A novel privacy preserving 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.

About authors :

Mr. KOLA SATISH KUMAR is a student of Raghu Engineering College, Dakamarri, VISAKHAPATNAM. He is presently pursuing his M.Tech degree from JNTU, Kakinada.

Mrs. ANURADHA TUTIKA is presently working as Assistant professor in CSE department, Raghu Engineering College, Dakarri, Visakhapatnam.

Mr. APPALA RAJU SAMANTHULA is presently working as Coordinator of the CSE department, Raghu Engineering College, Dakamrri, Visakhapatnam.