International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Authenticating Location Based Services with Spatial Query Processing

S.SURESH
Rajah Serfoji Government Arts College ,Tanjore

Dr.M. CHIDAMBARAM Msc, Mphil, MBA, PhD (Asst.Proff)
Rajah Serfoji Government Arts College,Tanjore

ABSTRACT:- *A moving kNN query continuously reports the k results (restaurants) nearest to a moving query point (tourist). In addition to the query results, a service provider often returns to a mobile client a safe region that bounds the validity of query results in order to minimize the communication cost between the service provider and that mobile client. However, when a service provider is not trustworthy, it may send inaccurate query results or incorrect safe regions to mobile clients. In this paper, proposed a framework for authenticating both the query results and the safe regions of moving kNN queries. It proved that the methods for authenticating moving kNN queries minimize the data sent between the service provider and the mobile clients. The proposed method can perform moving kNN query authentication with small communication costs and overhead.*

Keywords: **Query processing, security, integrity, and protection**

1. INTRODUCTION

Location-based services (LBSs) have been gaining tremendous popularity over the recent years, in particular since the emergence of mobile social networking services (mSNSs). Social networking giants such as Facebook and Twitter are all turning their services into mobile, along with specialized vendors like Foursquare, Gowalla and Loopt. Besides, major mobile carriers also strive to provide more value-added services to their subscribers, among which the most thrilling applications are LBSs such as location-aware advertisement ("check-in deals") and nearby-friend reminders. A typical LBS business model consists of a location registry (typically a social network or a mobile carrier who accepts user location updates or "check-ins"), a service provider (SP, typically a third party application developed on the social network) that offers LBS applications based on user locations, and a client (typically a mobile user) who requests the service. In this model, the third-party application is authorized to access user locations but it is not trustworthy regarding its service returned to the client. For example in Fig. 1, an SP offers location-based restaurant browsing which tells the client not only the nearby restaurants, but also the numbers of diners as an indication of their popularity. Each of these numbers can be retrieved by the SP through a spatial range query on a user location dataset specified by the client. However, the client may not trust these numbers as the SP has the motive to manipulate them in favor of "sponsored restaurants". As another example in public services, the government may outsource the online traffic monitoring service to third-party vendors. For market profits, however, they may prioritize the services by sending updated and accurate congestion reports to paid users while sending delayed or inaccurate ones to free users. These trustworthy issues are extremely important as more day-today businesses and public services are turning mobile and location-based. It would be soon indispensable for service providers to deliver their services in an authenticatable manner, in which the correctness

of service results — whether each result is genuine (soundness) and whether any result is missing (completeness) — can be verified by the client.

2. LITERATURE SURVEY

[1] H. Hacigumus, S. Mehrotra, and B. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.

The framework of data outsourcing was first introduced in , in which a data owner outsources its data to a third-party service provider who is responsible for answering the data queries from either the data owner or other users.

A new paradigm for data management in which a third party service provider hosts "database as a service" providing its customers seamless mechanisms to create, store, and access their databases at the host site. Such a model alleviates the need for organizations to purchase expensive hardware and software, deal with software upgrades, and hire professionals for administrative and maintenance tasks which are taken over by the service provider. Developed and deployed a database service on the Internet, called NetDB2, which is in constant use. In a sense, data management model supported by NetDB2 provides an effective mechanism for organizations to purchase data management as a service, thereby freeing them to concentrate on their core businesses. Among the primary challenges introduced by "database as a service" are additional overhead of remote access to data, an infrastructure to guarantee data privacy, and user interface design for such a service.

[2] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.

Outsourcing data to third party data providers is becoming a common practice for data owners to avoid the cost of managing and maintaining databases. Meanwhile, due to the popularity of location based services (LBS), the need for spatial data (e.g., gazetteers, vector data) is increasing exponentially. Two main challenges with outsourcing datasets is to keep the data private (from the data provider) and ensure the integrity of the query result (for the clients). Unfortunately, most of the techniques proposed for privacy and integrity do not extend to spatial data. Hence, recent studies proposed various techniques to support either privacy or integrity (but not both) on spatial datasets. In this paper, for the first time, propose a technique that can ensure both privacy and integrity for outsourced spatial data. In particular, a one-way spatial transformation method based on Hilbert curves is used, which encrypts the spatial data before outsourcing and hence ensures its privacy.

[3] B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. 30th Int'l Conf. Very Large Data Bases (VLDB'04), pp. 720-731, Aug. 2004.

Database outsourcing is an emerging data management paradigm which has the potential to transform the IT operations of corporations. This paper addresses the privacy threats in database outsourcing scenarios where trust in the service provider is limited. Specifically, analyze the data partitioning (bucketization) technique and algorithmically develop this technique to build privacy-preserving indices on sensitive attributes of a relational table. Such indices enable an untrusted server to evaluate obfuscated range queries with minimal information leakage.

[4] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l

Conf. Distributed Computing Systems (ICDCS'11), June 2011.

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only *boolean* search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straight forward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE).

[5] F. Chen and A. Liu, "SafeQ: Secure and Efficient Query Processing in Sensor Networks," Proc. IEEE INFOCOM'10, pp. 1-9, Mar. 2010.

The architecture of two-tiered sensor networks, where storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries, has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. However, the importance of storage nodes also makes them attractive to attackers. In this paper, SafeQ, a protocol that prevents attackers from gaining information from both sensor collected data and sink issued queries is proposed. SafeQ also allows a sink to detect compromised storage nodes when they misbehave. *To preserve privacy*, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their values. *To preserve integrity*, a new data structure called neighborhood chains that allows a sink to verify whether the result of a query contains exactly the data items that satisfy the query is proposed.

Objective

The main objective of the project is to

- Design a variant of inverted index that is optimized for multidimensional points, and is thus named the spatial inverted index (SI-index).
- To provide a method for successfully incorporating point coordinates into a conventional inverted index with small extra space, owing to a delicate compact storage scheme

- To calculate the distance between the query points and the nearest neighbour points using Haversine algorithm

Scope

The importance of spatial databases is reflected by the convenience of modeling entities of reality in a geometric manner. For example, locations of restaurants, hotels, hospitals and so on are often represented as points in a map, while larger extents such as parks, lakes, and landscapes often as a combination of rectangles. Many functionalities of a spatial database are useful in various ways in specific contexts. For instance, in a geography information system, range search can be deployed to find all restaurants in a certain area, while nearest neighbor retrieval can discover the restaurant closest to a given address.

3. PROBLEM STATEMENT: .

Existing techniques have been developed for a variety of queries, including relational queries, sliding window queries, spatial queries, text similarity queries, shortest path queries, moving kNN queries, moving range queries, and subgraph search. However, all existing Authenticated Data Structures (ADS) are either inapplicable or inefficient, since the authentication of *k*NN queries involves verifying both spatial proximity and text relevance. Moreover, authenticating an *k*NN query includes verifying both the top-k result and the accompanying safe zone. The safe zone is calculated based on both the objects in the top-k result and the objects not in the top-k result, so that missing a non-result object may cause a safe zone to fail in the authentication. Although authentication techniques for moving kNN queries and moving range queries involve safe zone verification, the safe zone of an *k*NN query is very different.

4. EXISTING SYSTEM:

- To meet the accuracy requirement, the framework SMashQ is used for the LBS to answer KNN queries accurately by retrieving live travel times (and routes) from online route APIs (e.g., Google Directions API, Bing Maps API, which have live traffic information.
- Indexing on road networks have been extensively studied in the literature. Various shortest path indices have been developed to support shortest path search efficiently.
- Papadias et al. study how to process range queries and KNN queries over points-of-interest, with respect to shortest path distances on a road network.
- Thomsen et al. study the caching of shortest paths obtained from online route APIs. They exploit the optimal subpath property on cached paths to answer shortest path queries.

DISADVANTAGES OF EXISTING SYSTEM:

- Query results with inaccurate travel times may disrupt the users' schedules, cause their dissatisfaction, and eventually risk the LBS losing its users and advertisement revenues.
- Similarly, high response time may drive users away from the LBS.
- As a remark, online maps (e.g., Google Maps, Bing Maps), on the other hand, cannot process queries for the LBS either, because those queries may involve specific attributes (e.g., quality, price, facility) that are only maintained by the LBS.
- SMashQ does not utilize route log to derive exact travel times nor lower/upper bounds to boost the query performance of the LBS.

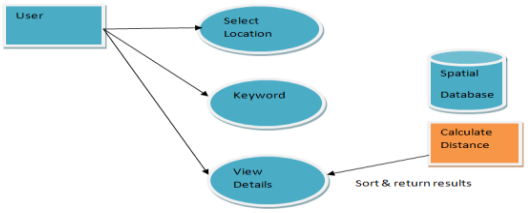
5.PROPOSED SYSTEM:

- In this paper, we exploit an observation namely that travel times change smoothly within a short duration. Routes recently obtained from online route APIs may still provide accurate travel times to answer current queries. This property enables us to design a more efficient solution for processing range and KNN queries.
- Specifically, our method Route-Saver keeps at the LBS the routes which were obtained in the past d minutes (from an online route API), where d is the expiry time parameter. These recent routes are then utilized to derive lower/upper bounding travel times to reduce the number of route requests for answering range and KNN queries.
- To reduce the number of route requests while providing accurate results, we combine information across multiple routes in the log to derive tight lower/upper bounding travel times. We also propose effective techniques to compute such bounds efficiently. Moreover, we examine the effect of different orderings for issuing route requests on saving route requests. And we study how to parallelize route requests in order to reduce the query response time further.

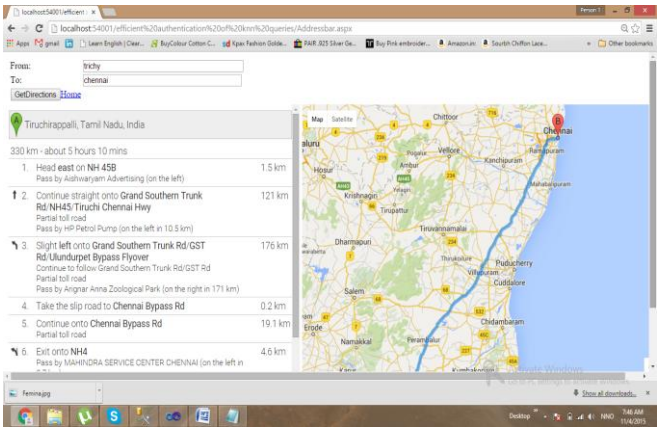
ADVANTAGES OF PROPOSED SYSTEM:

- Our experiments show that our solution is three times more efficient than SMashQ, and yet achieves high result accuracy (above 98 percent).
- Combine information across multiple routes in the log to derive lower/upper bounding travel times, which support efficient and accurate range and KNN search.
- Develop heuristics to parallelize route requests for reducing the query response time further.
- Evaluate our solutions on a real route API and also on a simulated route API for scalability tests.

6. SYSTEM MODEL



Screenshots:



8. CONCLUSION AND FUTURE WORK

Proposed an efficient method to authenticate moving kNN queries. Result proved that the method is VO-optimal, i.e., the verification object has the minimal size with respect to the given tree. Developed optimization techniques that can further reduce the computation cost, communication frequency and cost between a moving client and the LBS. Furthermore, extended the solution to handle moving kNN queries that involve multiple data sets. Experimental results show that the authentication method achieves low communication cost and CPU overhead. An interesting future work is to develop moving kNN query authentication technique for a location registry that manages mobile users' private locations. In this scenario, an additional requirement is to avoid disclosing non- result points to the query client . It is challenging to authenticate a safe region as its vertices and edges may allow an adversary to infer some non-result points.

9. REFERENCES:

1] H. Hacigumus, S. Mehrotra, and B. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.

[2] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.

[3] B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. 30th Int'l Conf. Very Large Data Bases (VLDB'04), pp. 720-731, Aug. 2004.

[4] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS'11), June 2011.

[5] F. Chen and A. Liu, "SafeQ: Secure and Efficient Query Processing in Sensor Networks," Proc. IEEE INFOCOM'10, pp. 1-9, Mar. 2010.

[6] An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data

[7] Authentication of Outsourced Databases using Signature Aggregation and Chaining