INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

ASSURANCE OF QUERY ACCESSING IN AN OUTSOURCED SPATIAL DATABASE MODEL

Athira.S.Kumar [1], **Dr.S.Uma** [2]

PG Scholar, PG CSE Department, Hindusthan Institute of Technology. Coimbatore,Tamil Nadu,India [1]

Head of the Department, PG CSE Department, Hindusthan Institute of Technology. Coimbatore,Tamil Nadu,India[2]

ABSTRACT: The concept of Query execution assurance is an important concept in the outsourced database point of view. We know that extending query execution assurance to the databases with multiple data owners is not at all efficient. In order to adapt with the lazy servers in the distributed scenario, we propose *efficient query access assurance* (EQAA) that focuses on IO-bounded queries. The goal in EQAA is to enable clients to verify that the server has a honest access to all the records that are inevitable to compute the accurate query answer, thus abrogating the bonuses for the server to be lazy if the total query cost is dominated by the IO cost in accessing these records. We reorganize this concept for distributed databases, and present efficient schemes that achieve EQAA with high success results. The scheme is easy to implement and deployment friendly, but may subject to excessive server overload for client communication cost and client side verification cost, when the query selectivity increases. EQAA produces significantly smaller verification objects (*VO*) and is more computationally efficient, especially for queries with low selectivity.

Keywords: Database as a service, database security, quality of services, query assurance.

I. INTRODUCTION

Many query authentication solutions have been proposed for auditing query results in an outsourced relational database in the assurance of various query results. The aim is to add authenticate the information into a spatial data structure by chains or by construction on the data points within each partition as well as on the partitions in the data space as well. For a given range query, this approach generates a proof that every data point ,within the intervals of the certified chains that overlap the query window is either returned as a result or falls outside the query range. Based on this, was designed a mechanism for authenticating kNN queries on multidimensional databases, ensuring that the result set is complete, authentic, and minimal. Both solutions incur significant authentication overhead, and the required verification information consumes considerable client-server communication bandwidth.

The main focus is on the Outsourced Spatial Databases. Query integrity assurance is an important and challenging problem that has to be carefully addressed. The LBS, if found untrusted can return incorrect or incomplete results. To differentiate from traditional type query, the term spatial query with an integrity assurance is verifiable query. In particular, for a spatial query, the client must be able to prove that the result set is correct. The framework commonly used in the literature for query integrity assurance is based on digital signatures and use a public-key cryptograhy, such as RSA. Initially, the DO obtains a private and a public key through a trusted key Distribution Centre. A private key is kept secret at the DO, whereas the public key is accessible publically. Using its private key, the DO uses digital signatures of the data by generating a number of signatures. It then sends the respective signature and the data to the SP which constructs the necessary data structures for efficient query processing.

II. EXISTING SYSTEM

In an industrial point of view, there are various existing systems that are to be considered while developing an optimal authentication system for query integrity assurance of the outsourced spatial databases of the various spatial queries. Some of them are discussed pointing out the drawbacks of the same.

A. Authentication of Location Based Skyline Queries

The work propose two authentication methods: one based on the traditional MR-tree index and the other based on a newly developed MR-Sky-tree. Spatial databases from various sources like traffic management, land surveys and environmental monitoring that are often outsourced to a service provider. An outsourcing model brings a great challenge in query processing. Since LBS is not the real owner of data, clients require to authenticate the soundness and completeness of the query results: soundness means that the original data is not modified by the LBS, while completeness means that no valid result is missing [9]. In this, it defines for each user query, in the LBS server to return the query results, the root signature, as well as a verification object (VO) that is constructed.

The correctness of the query results can be verified by the client using the returned VO, the root signature, and the DO’s public key for the authenticated processing of location-based queries. The existing approaches are confined to proximity-based queries, including range queries, k Nearest-Neighbor (kNN) queries, and shortest-path queries. These queries are not sufficient to the LBS applications that need to consider both spatial and non-spatial attributes of queried objects.

The limitations of the system are:

- The dynamic nature of spatial attributes makes location based skyline queries unique and challenging.
- The skyline results would be different with respect to different query locations. Several algorithms have been proposed to answer location-based skyline query
- No existing work has authenticated the processing of such queries.

B. Short Signatures Using Weil Pairing

The introduction of a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves[1]. The introduction of a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves is proposed . The length of signature is half the size of a DSA signature for a similar level of security. A short signature scheme is designed for systems where signatures are typed in by a human or signatures are sent over a low-bandwidth channel. Short digital signatures are needed in environments where a human is asked to manually key in the signature. .

It provides a level of security similar to 320-bit DSA signatures. But the signature scheme is secure only against existential forgery under a chosen message attack assuming the Computational Diffie Hellman problem (CDH) is hard on certain elliptic curves over a finite field. Generating a signature is a simple multiplication on the curve. The signature verification is done by using a bilinear pairing of the curve. This signature scheme inherently uses properties of elliptic curves. Consequently, there is no equivalent of scheme in Fp. The limitations of Weil pairing method for short signatures are:

- Due to the properties of the curves used, currently it can only provide signatures of the reduced lengths.
- The best known algorithm for solving the CDH problem in these groups requires a discrete-log on a finite field of characteristic tree.
- It can generate a signature of length 154 bits with security comparable to 320-bit DSA or 320-bit ECDSA only .
- Most Gap Diffie-Hellman groups are relatively long and do not lead to short signatures.

C. Providing Database As A Service

DaaS explores a new paradigm for data management in which a third party service provider hosts ”database as a service” methodology providing its customers seamless mechanisms for the creation, storage, and access to their databases at the host site itself. Such a model alleviates the need for organizations to purchase expensive hardware and software, deal with software upgrades, and need to hire professionals for administrative and maintenance tasks

It has developed and deployed a database service on the Internet, called NetDB2[4]. The data management model supported by NetDB2 provides an effective mechanism for organizations to purchase data management as a service, thereby making them free to concentrate on their core business. The main challenges that are introduced by “database as a service” are:

- Additional overhead of remote access to data provides an infrastructure to guarantee privacy of data, and UI design for such a service.
- Data privacy is a vital problem and proposes alternative solutions based on data encryption. .

- This strategy has been getting increasingly expensive and impractical as the database systems and problems become larger and more complicated.

III. PROPOSED SYSTEM

The proposed system is a secure spatial query integrity assurance method. The proposal for an EQAA framework that incorporates the accuracy and privacy issues. Here adapt for a monitoring region, the efficiency model that has been employed by use of location cloaking and other location based approaches. More specifically, a mobile client encapsulates its exact position in a voronoi box, and the timing and the other mechanism with which the box is updated to the server are decided by the client-side location updater as part of *Efficient Query Access Assurance (*EQAA).

The advantages are that it addresses the issue of location updating holistically with monitoring accuracy and privacy, and the updates are saved in a cache. It is concluded that by use of this approach location updates are greatly reduced to only when an object is moving out of the processing area. The safe region is specified by a voronoi box strategy that is determined by means of a Voronoi Diagram that is obtained from the underlying spatial datasets. Framework does not presume any kind of mobility pattern on moving clients.

A. Monitoring Clients in an OSDB

The assumption is that the clients are mobile users who issue location-based queries (eg: range queries), inorder to discover the points of interest (POIs) in their neighborhood region. There exist two major concerns with this model. First, as the Service Provider is not the real owner of the data, it might return incomplete results out of its own interest. Second, query results might have been tampered by malicious attackers who could substitute one or more records with fake ones.

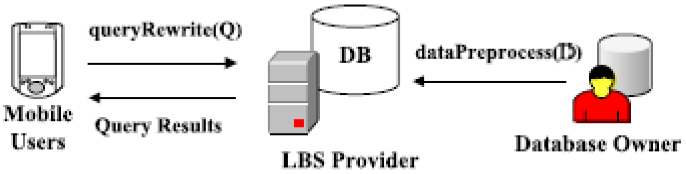

Fig.3.1: Spatial Data Outsourcing

Consequently, query integrity assurance is an important and challenging problem that has to be carefully addressed. To differentiate from a traditional query, the spatial query deals with integrity assurance as a verifiable query[5]. In particular, for a verifiable spatial query, the client must be able to prove that all the data returned from the server was originated at the DO and the obtained resultset after processing is correct and sound query result. The framework generally used in the literature for query integrity assurance is based on digital signatures and utilizes a public-key cryptographic method, such as RSA.

The Outsourced Spatial Database model is shown below in Fig.3.1. Firstly, the DO obtains a private and a public key through a trusted key distribution center. The private key is kept secret at the DO, whereas the public key is accessed by all the clients as shown.

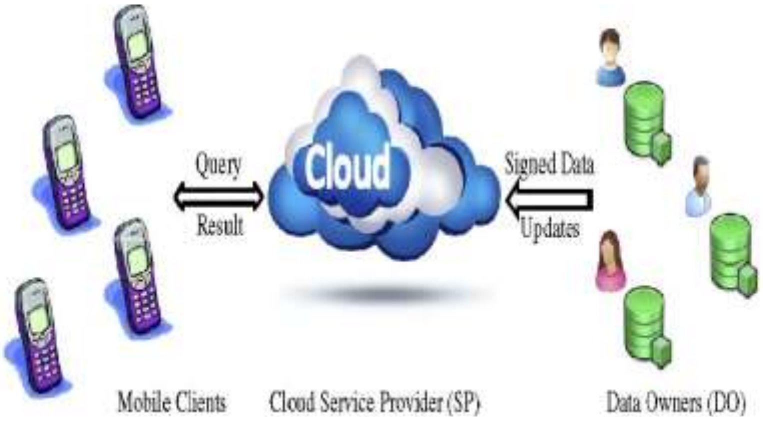

Fig.3.2: OSDB Data Model

B. Location Updation of the Mobile Clients

The system architecture of the proposed system is shown in figure 3.2. There is an index methodology followed in the proposed solution where there are two different indexing strategies used: Object Indexing for the Verification Object at the DO and Query Index at the subserver. The Query Processor processes these queries afer the user has registered on the network. The Location Manager updates the query index from the object index thereby following a geomeric verification of the location. A Voronoi box strategy is used in this approach my means of Voronoi diagram of the underlying databses for the processing of spatial queries. It has set forth a safe region limit for a mobile client. The clientside location updater updates the location and notifies the server only when it moves out of the box region. Thus,decrementing the number of database updates by using the strategy improves the eficiency of the query result using EQAA.

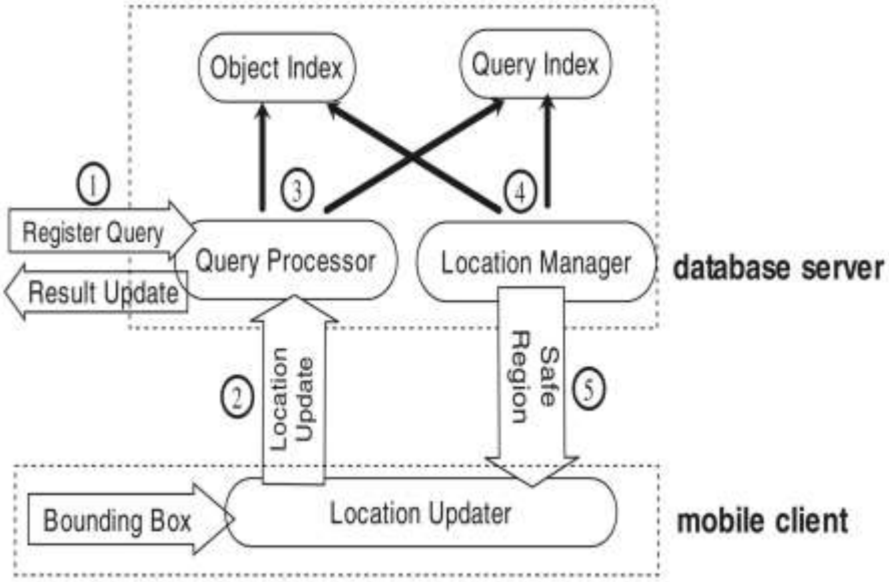

Fig.3.3: System Architecture

IV. CONCLUSION

The advantages of the proposed scheme overcomes most of the disadvantages discussed. The framework does not presume any mobility pattern on moving clients. The work aims to achieve the integrity of queries as well as query access assurance. The merits of EQAA are listed below:

- Addresses the issue of incomplete query results
- Minimal deployment cost
- Reduces database updates to only when an object is moving out of the voronoi box
- Framework does not presume any prior mobility pattern on mobile clients

The applications of the proposed system can be used for providing location based services (LBS) over outsourced databases on any type of mobile communication in the medical, business fields and other commercial fields of industry. Integrity assurance of various queries is provided with this approach as well as the correctness and completeness of the result set is dealt with.

Also future work is plan to incorporate other types of range queries into the framework, such as spatial joins and aggregate kNN queries is under development. There is a suggestion plan to optimize further the performance of the framework. In particular, the minimum database update cost strategy shows that voronoi box region is a crude approximation of the ideal safe region, mainly because the optimizations are carried on the safe region separately for each query, but not in a global scenario.

REFERENCES

[1] Boneh.D, Lynn.B, and Shacham.H, “Short Signatures from the Weil Pairing,” J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004. .

[2] Cheng ,W and K.-L. Tan, “Authenticating kNN Query Results in Data Publishing,” Proc. Fourth VLDB Conf. Secure Data Management, pp. 47-63, 2007. 874 IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 4, April 2013

[3] Guttman.A, “R-Trees: A Dynamic Index Structure for Spatial Searching,” Proc. ACM SIGMOD Int’l Conf. Management of Data,,pp. 47-57, 1984.

[4] Hacigu¨mu.H¨ s, Mehrotra.S, and Iyer.B.R, “Providing Database as a Service,” Proc. Int’l Conf. Data Eng. (ICDE), pp. 29-38, 2002.

[5] LinG Hu, W.-S. Ku, S. Bakiras, and C. Shahabi, “Verifying Spatial Queries Using Voronoi Neighbors,” Proc. 18th SIGSPATIAL Int’l Conf. Advances in Geographic Information Systems , pp. 350-359, 2010.

[6] Kolahdouzan.M.R and Shahabi.C, “Voronoi-Based K Nearest Neighbor Search for Spatial Network Databases,” Proc. 30th Int’l Conf. Very Large Data Bases (VLDB), pp. 840-851, 2004.

[7] Ku.W.S, L. Hu, C. Shahabi, and H. Wang, “Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases,” Proc. 11th Int’l Symp. Advances in Spatial and Temporal Databases (SSTD), pp. 80-97, 2009.

[8] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, “Dynamic Authenticated Index Structures for Outsourced Databases,” Proc. ACM SIGMOD Int’l Conf. Management of Data,, pp. 121-132, 2006.

[9] Lin.X, Xu.J, and Hu.H, “Authentication of Location-Based Skyline Queries,” Proc. 20th ACM Int’l Conf. Information and Knowledge Management (CIKM), pp. 1583-1588, 2011

BIOGRAPHY

Athira S Kumar

She received the B.Tech degree in Computer Science & Engineering from College Of Engineering, Adoor, Kerala in 2012. She is currently doing the M.E. in Computer Science and engineering in Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, now working on the research project in Data mining.

Dr.S.Uma is Professor and Head of the PG Department of Computer Science and Engineering at Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India. She received her B.E., degree in Computer Science and Engineering in First Class with Distinction from P.SG. College of Technology in 1991 and the M.S., degree from Anna University, Chennai, Tamil Nadu, India. She received her Ph.D., in Computer Science and Engineering from Anna University, Chennai, Tamil Nadu, India with High Commendation. She has nearly 23 years of academic experience. She has organized many National Level events like seminars, workshops and conferences. She has published many research papers in National and International Conferences and Journals. She is a potential reviewer of International Journals and life member of the ISTE professional body. Her research interests are pattern recognition and analysis of nonlinear time series data.