ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Privacy and Accuracy Monitoring Of Spatial Queries Using Voronoi Neighbors Using Data Mining

Athira.S.Kumar [1], Dr. S.V.M.G.Bavithiraja [2]

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

Assistant Professor, Department of CSE, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu,India[2]

ABSTRACT: The approach is based on neighborhood information derived from the Voronoi diagram of the underlying spatial data set and can handle fundamental spatial query types. It opts for a monitoring environment, the privacy model that has been employed by location cloaking and other privacy-aware approaches. The idea is that a client encapsulates its exact position in a bounding box, and the timing and mechanism with which the box is updated to the server are decided by a client-side location updater as part of PAM.

KEYWORDS: MR Tree, VN Auth, Bounding Box, Location Cloaking, Outsourced Databases, Voronoi Diagram

I. Introduction

The idea of outsourcing databases to a third-party service provider was introduced, as a result of which, numerous query authentication solutions have been proposed for auditing query results in outsourced relational databases. The first mechanism for verifying query results in multidimensional databases was proposed. The aim is to add authentication information into a spatial data structure by constructing certified chains on the data points within each partition as well as on all the partitions in the data space.

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 focus is on the Outsourced Spatial Database (OSDB) model. The assumption is that the clients are mobile users who issue location-based queries (e.g., k nearest neighbor (kNN) or range queries), in order to discover points of interest (POIs) in their neighborhood. There exist two major concerns with this model. First, as the SP is not the real owner of the data, it might return dishonest results out of its own interests. Second, query results might be tampered with by malicious attackers who could substitute one or more records with fake ones.

Query integrity assurance is an important and challenging problem that has to be carefully addressed. To differentiate from traditional queries, the term spatial queries with integrity assurance is verifiable query. In particular, for a verifiable query, the client must be able to prove that 1) all data returned from the SP originated at the DO and 2) the result set is correct and complete.

The general framework commonly used in the literature for query integrity assurance is based on digital signatures and utilizes a public-key cryptosystem, such as RSA. Initially, 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 accessible by all clients. Using its private key, the DO digitally signs the data by generating a number of signatures. Then, it sends the signatures and the data to the SP which constructs the necessary data structures for efficient query processing. When the SP receives a query from a client, it generates a verification object (VO) that contains the result set along with the corresponding authentication information. Finally, the SP sends the VO to the client which can verify the results using the public key of the DO

II. EXISTING SYSTEM

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

A. Authentication of Location Based Skyline Queries

In outsourced spatial databases, the location-based service (LBS) provides query services to the clients on behalf of the data owner. If the LBS is not trustworthy, it may return incorrect or incomplete query results. Thus, authentication is needed to verify the soundness and completeness of query results.The authentication problem for location-based skyline queries, which have recently been receiving increasing attention in LBS applications. 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[8]. Experimental results demonstrate the efficiency of our proposed methods in terms of the authentication cost.

The past decade has seen tremendous amount of research efforts in spatial database technology. Spatial databases from various sources (e.g., land surveys, traffic management, and environmental monitoring) are often outsourced to a service provider (i.e., LBS)[7] because the agencies collecting such data e.g., governments or non-profit organizations are usually not able to support advanced query services. Such an outsourcing model brings a great challenge in query processing. Since the LBS is not the real owner of data, clients may want to authenticate the soundness and completeness of query results: soundness means that the original data is not modified by the LBS, while completeness means that no valid result is missing. The situation leads to a problem known as authenticated query processing. A general framework of authenticated query processing is dealt with[9]. Before outsourcing a spatial dataset to the LBS, the data owner (DO) builds an authenticated data structure (ADS) of the dataset.

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 signature length 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. For example, product registration systems often ask users to key in a signature provided on a CD label. More generally, short signatures are needed in low-bandwidth communication environments. For example, short signatures are needed when printing a signature on a postage stamp. Currently, the two most frequently used signatures schemes, RSA and DSA, provide relatively long signatures compared to the security they provide.

For example, when one uses a 1024-bit modulus, RSA signatures are 1024 bits long. Similarly, when one uses a 1024-bit modulus, standard DSA signatures are 320 bits long. Elliptic curve variants of DSA, such as ECDSA, are also 320 bits long. A 320-bit signature is too long to be keyed in by a human. The signature scheme whose length is approximately 160 bits provides a level of security similar to 320-bit DSA signatures. The signature scheme is secure 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 of characteristic three. Generating a signature is a simple multiplication on the curve. Verifying the signature is done using a bilinear pairing on the curve. This signature scheme inherently uses properties of elliptic curves.

C. Providing Database As A Service

Explore 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. There has developed and deployed a database service on the Internet, called NetDB2, which is in constant use[4]. The 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. These issues are investigated in the study.

III. PROPOSED SYSTEM

The proposed system is a secure way of preserving the spatial query integrity. The proposal for a privacy and monitoring framework that incorporates the accuracy, efficiency, and privacy issues altogether. Here adapt for the monitoring environment ,the privacy model that has been employed by location cloaking and other privacy-aware approaches. More specifically, a client encapsulates its exact position in a bounding box, and the timing and mechanism with which the box is updated to the server are decided by a client-side location updater as part of PAM.

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

A. Outsourcing the Database and Monitoring Clients

The assumption is that the clients are mobile users who issue location-based queries example, k nearest neighbor (kNN) or range queries, in order to discover points of interest (POIs) in their neighborhood. There exist two major concerns with this model. First, as the SP is not the real owner of the data, it might return dishonest results out of its own interests. Second, query results might be tampered with by malicious attackers who could substitute one or more records with fake ones.

Consequently, query integrity assurance is an important and challenging problem that has to be carefully addressed. To differentiate from traditional queries, the term spatial queries deals with integrity assurance as verifiable queries[6]. In particular, for a verifiable query, the client must be able to prove that 1) all data returned from the SP originated at the DO and 2) the result set is correct and complete.The general framework commonly used in the literature for query integrity assurance is based on digital signatures and utilizes a public-key cryptosystem, such as RSA .

The Outsourced Spatial Database (OSDB) model, as shown in Fig.3.1. Initially, 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 accessible by all clients as shown in the figure. Using its private key, the DO digitally signs the data by generating a number of signatures. Then, it sends the signatures and the data to the SP which constructs the necessary data structures for efficient query processing. When the SP receives a query from a client, it generates a verification object (VO) that contains the result set along with the corresponding authentication information. Finally, the SP sends the VO to the client which can verify the results using the public key of the concept.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

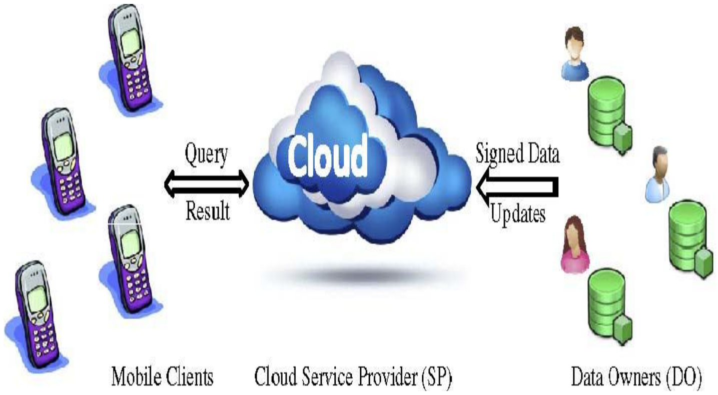

Fig.3.1: Query Processing with DO

B. Geometric Verification and Location Updater

The system architecture of the proposed system is shown in figure 3.2. There is an index methodology followed in this view.There are two indexes used: Object Index and Query Index.The Query Processor processes these queries afer the user has registered in the network.The Location Manager updates the query index from the object index thereby following a geomeric verificaion.A bounding box strategy is used in this approach.The bounding box set forth the safe region limits of a client using the underlying spatial datsets using Voronoi Diagram.The clientside location updater updates the location and notifies the server only when it moves out of the safe region.Thus,decrementing the data updates by using the strategy improves the eficiency of the query result.

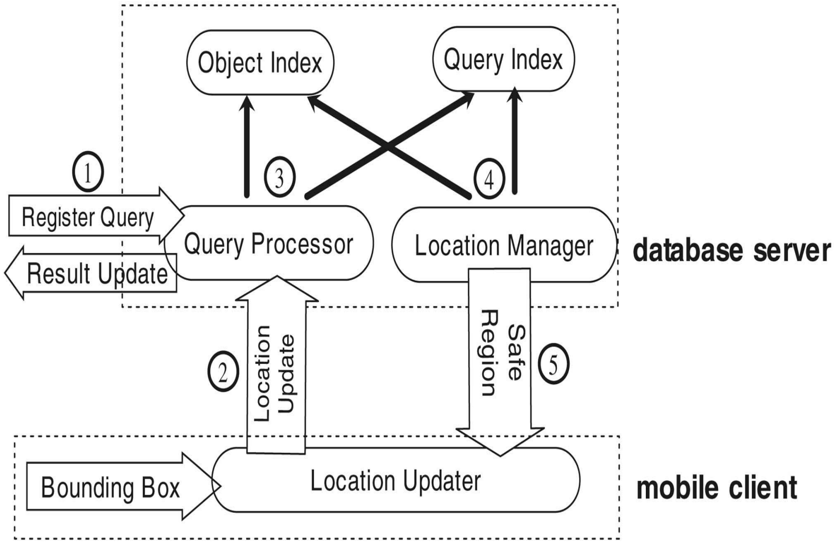

Fig.3.2 System Architecture

IV. CONCLUSION

The advantages of the system proposed overcomes most of the disadvantages discussed .The framework does not presume any mobility pattern on moving objects. The work aims to achieve the geometric verification of the queries as well as location updation. The merits are listed below:

- Addresses the issue of location updating holistically with monitoring accuracy, efficiency, and privacy altogether.
- Minimal communication cost.
- Reduces location updates to only when an object is moving out of the safe region.
- Framework does not presume any mobility pattern on moving objects.

The applications of the proposed system can be used for providing location based services over outsourced databases on any type of Mobile communication in the business fields, medical,and other commercial fields of industry. Query integrity assurance is provided with this approach as well as the correctness and completeness of the resultset is dealt with. Privacy of the query resultset is guaranteed by means of Privacy and Monitoring PAM by help of Voronoi Neighbors**.**

Also a future enhancement plan to incorporate other types of queries into the framework, such as spatial joins and aggregate queries is under research. There is also plan to further optimize the performance of the framework. In particular, the minimum cost update strategy shows that the safe region is a crude approximation of the ideal safe area, mainly because separate optimizations are carried on the safe region for each query, but not globally.

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

Mrs S.V.M.G. Bavithiraja was born in Madurai, Tamilnadu,India on May 31,1980. She obtained her B.E. (CSE) from Madurai Kamraj University, Madurai, , India in 2002 and received her Master of Computer Science and Engineering from Anna University,Chennai, India in 2008.She is currently a lecturer in Hindusthan Institute ofTechnology, Coimbatore, India. She received her Ph.D research interests in WiMAX (World Wide Interoperability for Microwave Access) and Wireless Sensor networks.