INTACT: A Spatial Query Integrity Assurance Framework for Location-based Services (Demo Paper)

Chih-Jye Wang
Dept. of CSSE
Auburn University
Auburn, AL, USA
wangchj@auburn.edu

Wei-Shinn Ku
Dept. of CSSE
Auburn University
Auburn, AL, USA
weishinn@auburn.edu

Ling Hu
Computer Science Dept.
Univ. of Southern Cal.
Los Angeles, CA, USA
lingh@usc.edu

Cyrus Shahabi
Computer Science Dept.
Univ. of Southern Cal.
Los Angeles, CA, USA
shahabi@usc.edu

ABSTRACT

It is cost-effective for data owners to publicize their spatial databases via database outsourcing; however, data privacy and query integrity are major challenges. In this demonstration, we implemented the INTACT (spatial query INTegrity AssuranCe framework for locaTion-based services) framework on the iPhone and the .NET Framework that protects data privacy using space encryption and ensures query integrity via audit queries.

Categories and Subject Descriptors

H.2.8 [**Database Management**]: Database Application—*spatial databases and GIS*

General Terms

Algorithms and Experimentation

Keywords

Spatial database outsourcing, location-based services

1. INTRODUCTION

In supporting ubiquitous and instantaneous access of critical information, more spatial data owners are publishing their datasets on to the Cloud through database outsourcing [1], by which critical data can reach large number of audiences dispersed geographic regions. As an example, *during* the Gulf of Mexico oil spill in 2010, the US Coast Guard (a data owner) collects the coverage of the affected area and outsources that data to a location-based service (LBS) provider, for example Google, so that the clients of the LBS, such as marine-based organizations operating in the area, could stay away from the affected area. The motivation for spatial data outsourcing is cost-effectiveness of providing the spatial data. LBS providers have the infrastructure to cost-effectively provide the data to a large number of clients.

To keep the data private and ensure the integrity of the query result are the major challenges of spatial database outsourcing. Ku et al. [3] proposed a technique that can ensure both privacy and integrity for outsourced spatial databases. With the solution in [3], the database owner first employs a one-way spatial transformation method to encrypt the spatial data before outsourcing and hence ensures its privacy. Afterward, a percentage of the original database is replicated and encrypted with a different encryption key. Query results are validated via audit queries based on the replicated portion of the database.

This demonstration presents INTACT - a novel framework which protects both privacy and integrity of outsourced spatial databases by space encryption [2] and audit queries. INTACT supports both k Nearest Neighbor (kNN) and spatial range queries, the building blocks of any LBS application. We implement the LBS server on .NET Framework Web Services and the clients on iPhone SDK 3.2.

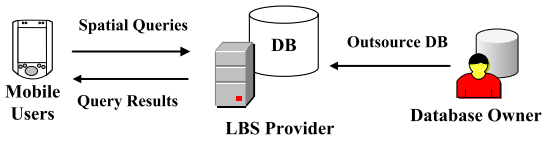

Figure 1: The INTACT framework architecture.

2. INTACT FRAMEWORK

2.1 Architecture

The architecture of our INTACT framework is depicted in Figure 1 which contains three components: mobile user, LBS provider, and database owner. Mobile users send their spatial queries to the LBS provider which evaluates the queries by accessing the outsourced database prepared by the database owner. However, the LBS provider could be malicious (e.g., returning incomplete query results) and it is not trusted by the other two components.

2.2 Approach Overview

The database owner employs the Hilbert curve based space encryption mechanism to protect data privacy. Prior to outsourcing, the database owner first replicates a portion of the original dataset with randomly selected objects and then encrypts the original dataset with the primary space encryption key, SEK_P, and the duplicated dataset with the secondary encryption key, SEK_S. Afterward, the two encrypted datasets are combined and stored at the LBS provider. The encryption keys are ultimately shared with all clients, allowing the clients to launch both spatial queries and audit queries. By exploiting the replicated data, clients are able to determine if the LBS provider is honest.

2.3 Range Query

With a given range query Q_R, a client utilizes the SEK_P to identify all the Hilbert values that are covered by Q_R and sends the Hilbert values to the LBS provider for retrieving the objects

ACM GIS'10, November 2-5, 2010. San Jose, CA, USA

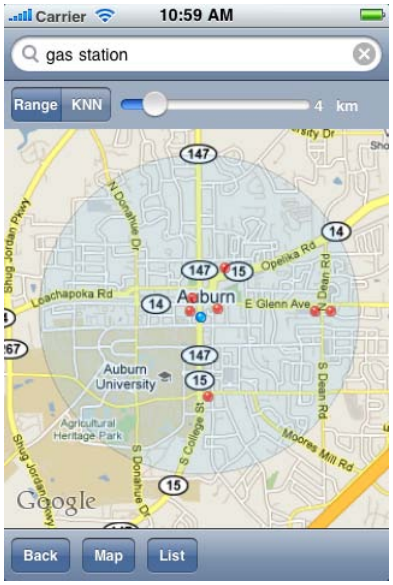

Figure 2: Range query result.

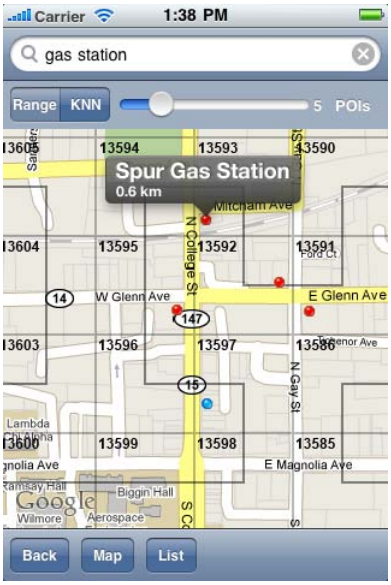

Figure 3: kNN query result with the Hilbert curve.

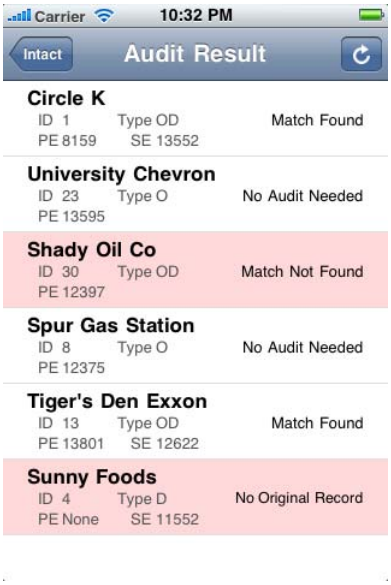

Figure 4: Audit query result.

covered by the query range. The client filters out duplicated objects (encrypted with SEK_S) and the remaining objects are the range query result.

2.4 k Nearest Neighbor Query

For a given kNN query point q, a client first employs SEK_P to compute the Hilbert value of q as the query point in the encrypted space. Afterward, the client transmits the rewritten query to the LBS provider for retrieving the query result set $\mathbb{R}$. Because of loss of a dimension in the encrypted space, the objects in $\mathbb{R}$ may not precisely match the actual k nearest neighbors of q. To compensate this, the client retrieves the object which has the longest distance d to q in $\mathbb{R}$ and utilizes d as a *search upper bound* for launching a range query Q_R with d to decide the query window size. Finally, the client has to identify the top k objects in the result set of Q_R based on their distance to q to acquire the final kNN query result.

2.5 Audit Query Composition

After each range query Q_R, the client has the option of issuing an audit query. An audit query is indistinguishable from regular queries and its purpose is to assess the honesty of the LBS provider. Note that kNN query is transformed to range query as described in the previous subsection. Therefore, we are able to audit kNN query with the same procedure.

To assure range query integrity, the client generates an audit range query Q_A with the same query range size as Q_R and the parameters of SEK_S (instead of SEK_P). If the service provider carries out Q_R honestly, the query result set of the audit query must contain counterparts of all the objects with duplicates in the query result set of Q_R.

3. DEMONSTRATION

3.1 Location-Based Service Server

The LBS server is implemented via Microsoft .NET Framework Web Services and invoked using HTTP based JavaScript Object Notation (JSON) messages. The Web service supports two interfaces: [GetRange(lower, upper)], and [GetNearestK(Hc, k)] that gets POIs at a range and nearest k, respectively.

3.2 Client

The client in this demo is implemented on the iPhone (SDK 3.2). Figure 2 illustrates the map view of the result of the range query in relation to the current location of the client. The blue dot and the blue circle signify the location of the client and the range of the query, respectively. The red pins signify the result POIs.

In addition to query result, the GUIs also illustrate the space encryption process. Figure 3 illustrates the query result of a kNN query. The black grid and the curve represent the Hilbert curved based space encryption that is used to conceal the locations of the spatial objects. For example, for the selected POI, its spatial location is mapped to 13593 in the database. The GUI allows the user to show neither, or both of the space encryption curves (primary and secondary).

Figure 4 shows an audit query result. For example, Sunny Foods in the figure is a record with duplicate, but the original record is not found. Therefore, it is resulting in the server flagged as untrusted.

4. CONCLUSIONS

The INTACT framework protects data privacy by masking the location of spatial data with the Hilbert curve based space encryption. To assure query integrity, our framework duplicates a percentage of the outsourced spatial database and encrypts the data using two space encryption keys. Our iPhone mobile client interacts with our LBS server for launching regular and audit queries to demonstrate the novel features of the INTACT framework.

Acknowledgments

This research has been funded in part by the National Science Foundation grants CNS-0831502 (CT) and CNS-0855251 (CRI).

5. REFERENCES

[1] H. Hacigümüs, S. Mehrotra, and B. R. Iyer. Providing database as a service. In *ICDE*, pages 29–38, 2002.

[2] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *SSTD*, pages 239–257, 2007.

[3] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang. Query Integrity Assurance of Location-based Services Accessing Outsourced Spatial Databases. In *SSTD*, pages 80–97, 2009.