isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 3 ,May,2016 ,ISSN_NO: 2321-3337

SIGNED SUBSPACE SKYLINE SCOPE AUTHENTICATED METHOD FOR SKYLINE QUERIES

Mrs.G.Rajalakshmi[1,] Mrs.B.Vijaya Nirmala[2]

PG Scholar, R.V.S Educational Trust's Group of Institution, Dindigul[1]
Assistant Professor, R.V.S Educational Trust's Group of Institution, Dindigul[2]

ABSTRACT**—** *A Novel idea for Merkle Skyline R-Tree Method and Novel Partial S4 Tree Method is proposed to authenticate one shot Location based Arbitrary subspace Skyline Query's (LASQs). MSR Tree authentication method is proposed for skyline query authentication. A continuous skyline query processing strategy is implemented for moving query points. Cloud Service Provider is responsible for maintaining the database. Query integrity assurance is based on digital signatures and utilizes a public key cryptosystem, such as RSA. The purpose of this project is to identify the location of moving client. Verification Object creation is proposed to verify the location and produce result to client. Client results are viewed through the geomap, which is based on road network map type.*

Keywords— Location based arbitrary subspace skyline query, query authentication, similarity search.

1. INTRODUCTION

1.1 LOCATION BASED SERVICES

Users carrying location aware mobile devices are able to query LBSs for surrounding points of interest (POIs) anywhere and at any time. Among the many types of location based queries, one important class is location based skyline queries. These skyline queries called location based arbitrary subspace skyline queries (LASQs). To scale up LBSs along with their ever growing popularity, a rising trend is to outsource data management and service provisioning to Cloud service providers (CSPs) such as Amazon EC2 and Google App Engine. The data owner obtains, through a certificate authority a pair of private and public keys of digital signatures. Before delegating a spatial dataset to the CSP, the data owner builds an authenticated data structure (ADS) of the dataset. To support efficient query processing, the ADS are often a tree like index structure, where the root is signed by the data owner private key. The CSP keeps the spatial dataset, as well as the ADS and its root signature. Upon receiving a query from the client, the CSP returns the query results, the root signature, and a verification object (VO), which is constructed based on the ADS. The client can authenticate the correctness of the query results using the returned VO, the root signature, and the data owner public key.

To extend this study to the general problem of authenticating location based skyline queries in arbitrary subspaces of attributes (LASQs). Because a basic solution that returns all results in the full space is inefficient, it propose a new authentication method based on the notion of signed sub space skyline scope (S4). It construct a data structure, called Partial S4 tree, which pre computes, signs, and stores the skyline scopes of some subspaces, so that many redundant objects can be easily identified and safely removed from the VO, thereby minimizing its size and saving the server processing time. To improve the filtering effects, it further proposes a storage budget allocation policy to construct the Partial S4 tree for each spatial object. For continuous LASQs, the concept of clear area is introduced to enable a moving client to re evaluate new results locally.

1.2 GEOMAP

A Geomap is a map of a country, continent, or region map, with colors and values assigned to specific regions. Values are displayed as a color scale, and can specify optional hover text for regions.

Data Format

Geomap supports two address formats.

Format 1: Latitude/Longitude locations

This format works only when the data mode option is markers. If this format is used, do not need to include the Google Map JavaScript. The location is entered in two Latitude/Longitude locations.

- [Number, Required] Latitude. Positive numbers are north, negative numbers are south.
- [Number, Required] Longitude. Positive numbers are east, negative numbers are west.
- [Number, Optional] A numeric value displayed when the user hovers over this region.
- [String, Optional] Additional string text displayed when the user hovers over this region.

Format 2: Address, country name, region name locations, or US metropolitan area codes

This format works with the data mode option set to either markers or regions. The location is entered in one column, plus two optional columns:

1. [String, Required] A map location. The following formats are accepted:
- A specific address (for example, "1600 Pennsylvania Ave").
- A country name as a string (for example, "England"), or an uppercase ISO-3166 code or its English text equivalent (for example, "GB" or "United Kingdom").

2. [Number, Optional] A numeric value displayed when the user hovers over this region.
3. [String, Optional] Additional string text displayed when the user hovers over this region.

1.3 MSR TREE

- Ensures Authenticity of the document as well as the schema.
- Associate a hash value with each node in the graph representation of the XML document.
- The hash value of a node is obtained by applying a hash function over the concatenation of its children.
- The hash values are computed using the Merkle Hash Function.

A hash tree is a tree of hashes in which the leaves are hashes of data blocks in, for instance, a file or set of files. Nodes further up in the tree are the hashes of their respective children. For example, in the picture hash 0 is the result of hashing the result of concatenating hash 0-0 and hash 0-1.

Hash 0 = hash (hash 0-0 + hash 0-1) where + denotes concatenation.

In the top of a hash tree there is a *top hash* (or *root hash* or *master hash*). Before downloading a file on a p2p network, in most cases the top hash is acquired from a trusted source, for instance a friend or a web site that is known to have good recommendations of files to download.

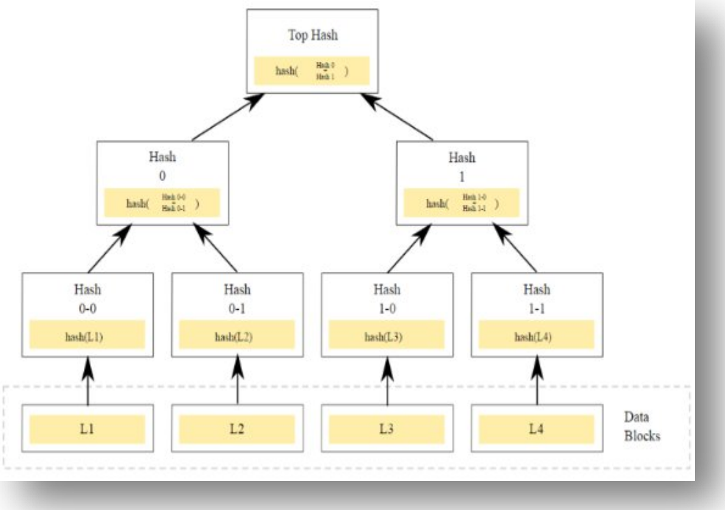

Figure.1 Merkle Hash Tree

When the top hash is available, the hash tree can be received from any non-trusted source, like any peer in the p2p network. Then, the received hash tree is checked against the trusted top hash, and if the hash tree is damaged or fake, another hash tree from another source will be tried until the program finds one that matches the top hash.

2. SYSTEM ANALYSIS

2.1 Existing System

Subgraph similarity search is used in graph databases to retrieve graphs whose subgraphs are similar to a given query. Filtering and Verification framework is the authenticated subgraph similarity search technique. Graph Metric Tree forms the basic authentication algorithm. Transform the similarity search into a search in a graph metric space and derive small verification objects (VOs) to be transmitted to query clients. Sampling based pivot selection method and an authenticated version of MCS is used to optimize GM Tree.

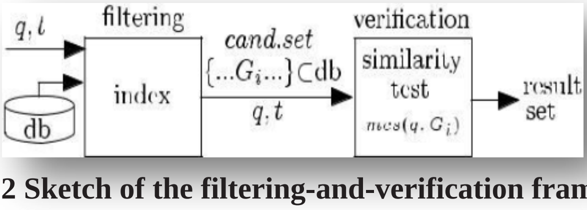

Figure.2 Sketch of the filtering-and-verification framework

The data owner publishes its database, index and signature to an SP. The SP processes queries from a client and returns to the client both the query result and a verification object (VO) which often encodes query processing traces such as index traversals. Using the query result and the VO, the client constructs the digest of the database/index and compares it with the signature of the data owner to authenticate the query result. As the filtering-and-verification framework is not specially designed for query authentication, we note that a naive application of existing query authentication techniques leads to at least three problems. No previous index specifically considered whether the candidate graphs were located together in the graph database, which directly affects the VO needed.

For instance, candidate and non-candidate graphs may be alternately stored in the database; and in this scenario, each candidate graph needs an item in the VO to authenticate that no candidate has been missed. As the number of candidate graphs for similarity search can be large, the VO for authenticating them can also be large. Second, one performance bottleneck at the client side is the distance computation on large candidate graphs, since the distance computation time is exponential to the graph size. Unfortunately, most existing approaches index similarity search by features or sub-graphs. The larger the graph is, the more features/subgraphs are there for indexing. Thus, large graphs are often included in candidate graphs. Third, clients are required to perform the costly subgraph similarity computation numerous times in order to authenticate the processing traces at the SP. Since such computation has already been done once at the SP, it is inefficient for the client to redo it from scratch.

2.2 Proposed System

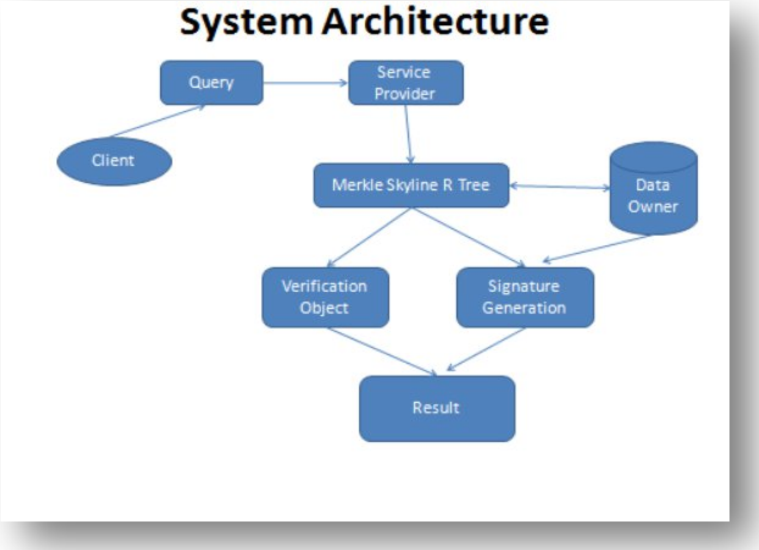

Figure.3 System Architecture

Merkle Skyline R-tree method and a novel Partial S4 tree method is used to authenticate one shot LASQs. Merkle Skyline R-Tree takes location as a root node. Partial S4 tree method pre computes, signs, and stores the skyline scopes of some subspaces, so that many redundant objects can be easily identified and safely removed from the VO Tree. Storage budget allocation policy is used to construct the Partial S4 tree for each spatial object. Query integrity assurance is based on digital signatures and utilizes a public key cryptosystem, such as RSA. Verification Object Tree construction helps to identify the client location and produce correct result.

3. IMPLEMENTATION STEPS

3.1 QUERY PROCESSING

A number of algorithms have been developed since then. These algorithms can be divided into two categories. The first category is non index based algorithms. The representatives are Block Nested Loop (BNL) and Divide and Conquer (D&C). The CSP may return incorrect results unintentionally because of bugs in the implementation of query processing algorithms. The CSP may intentionally tamper with the query results. The other category of skyline algorithms is index based. A high dimensional dataset is converted into a one dimensional dataset and a B + tree is built to accelerate query processing.

3.2 SIGNATURE GENERATION

Identify the problem of authenticating LASQs in outsourced databases. To the best of our knowledge, this study is the first attempt to investigate this problem. We developed new schemes for range and top k query authentication that preserves the location privacy of queried objects. The data owner obtains, through a certificate authority, a pair of private and public keys of digital signatures. Before delegating a spatial dataset to the CSP, the data owner builds an authenticated data structure (ADS) of the dataset. To support efficient query processing, the ADS is often a tree like index structure, where the root is signed by the data owner using private key. The CSP keeps the spatial dataset, as well as the ADS and its root signature. Upon receiving a query from the client, the CSP returns the query results, the root signature, and a verification object (VO), which is constructed based on the authenticated data structure. The client can authenticate the correctness of the query results using the returned verification object, the root signature, and the data owner’s public key.

3.3 MSR TREE GENERATION

Merkle Skyline R tree method and a Partial S4 tree method, aiming to reduce the server processing time and minimize the VO size. The root is b’s full space skyline scope, which serves as a data entry in the original MSR tree. Each edge in the Partial S4 tree is labeled with the attribute(s) by which the subspaces of the parent and the child node differ. The final VO is composed of: 1) the VO tree constructed based on the full-space MSR tree (excluding the redundant objects and their full space skyline scopes (So,$_{\wedge}$’s)); 2) the subspace skyline scopes (So,$_{\wedge}$’’s) of all redundant objects and their aggregate signature.

3.4 LASQ AUTHENTICATION

LASQ authentication method is introduced to support query authentication. The digest of each index node can be computed recursively in a bottom up fashion. Finally, the digest of the root node is computed and signed by the data owner using private key to generate the root signature. Hereafter, this authenticated index structure is called Merkle Skyline R tree. With the help of MSR-tree, an LASQ is reduced to a point location query on the indexed subspace skyline scopes. Specifically, starting from the root and going all the way down to the leaf nodes, the server checks whether any child of a node covers the query point. If it does, the node is unfolded and inserted into the VO for further checking; otherwise, the node is pruned and only its MBR and digest are inserted into the final VO. When visiting a leaf entry associated with an object t_o, if the corresponding S_o does not cover the query point, both S_o and H_o should be inserted into the VO; otherwise, *o* is an LASQ result and only So is inserted into the VO (H_o can be computed locally by the client based on the received result). It is noteworthy that as the nodes in the VO also form a tree structure, we call it a VO tree.

4. CONCULSION AND FUTUREWORK

The system focuses the problem of authenticating location based Arbitrary subspaces skyline Queries (LASQs). MSR Tree authentication method was proposed successfully for skyline query authentication. To enable authentication for large scale datasets and subspaces, further implementation of Partial S4 tree method, in which most of the redundant objects can be easily identified and filtered out from the VO. Query integrity assurance is successfully performed through public key cryptosystem. Partial S4 tree method is outperforms the basic authentication method by up to 69% in terms of the overall query latency and up to 74% in terms of the VO size. Extensive experimental results demonstrate the efficiency of proposed methods. Since the query distance is defined by network distance in a road network, the skyline scope defined in this paper no longer works, which calls for new authentication methods. Moreover, we are also interested in studying the authentication problem for dynamic objects, where how to guarantee the freshness of query results is a very challenging issue.

REFERENCES

[1] Beckmann N. Kriegel H.P. Schneider R. and Seeger B. (1990), The R*-tree: An efficient and robust access method for points and rectangles.

[2] Chen Q. Hu H. and Xu J. (2013), VERDICT: Privacy-preserving authentication of range queries in location-based services.

[3] He H. and Singh A. K. (2006), Closure-tree: An index structure for graph queries.

[4] Huang Z. Lu H. Ooi B. C. and Tong K. H. (2006), Continuous skyline queries for moving objects.

[5] Hu H. Xu J. and Lee D.L. (2005), A generic framework for monitoring continuous spatial queries over moving objects.

[6] Ku W.S. Hu L. Bakiras S. and Shahabi C. (2013), Spatial query integrity with voronoi neighbors.

[7] Kundu A. and Bertino E. (2010), How to authenticate graphs without leaking.

[8] Pang H. Jain A. and K Tan K.L. (2005), Verifying completeness of relational query results in data publishing.

[9] Yuanyuan T. Carlos C. S. States D. J. and Patel J. M. (2007), SAGA: A subgraph matching tool for biological graphs.

[10] Zhu Y. Qin L. Yu J.X. and Cheng H. (2012), Finding top-k similar graphs in graph database.