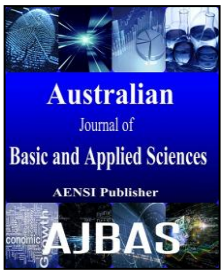
ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



Skyline Query Endorsement on Unsecure Location

[1]R. Geetha and [2]Dr. K.latha

[1]*PG Scholar, Department of CSE, Anna University, BIT Campus, Trichy, India.*
[2]*Assistant Professor, Department of CSE, Anna University, BIT Campus, Trichy, India.*

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
Location Based Services, Geo Spatial Information, mutable order preserving encoding, Advanced Encryption Standard.

ABSTRACT

Authentication on Location based services contributes major process of extracting queries on to client.While increasing data intensity in cloud may also need to improve scalability and stability. So it must preserve securely on violating environment. To taking spatial queries to perform client side points of interest. Propose a family of cryptographic technique that allow dealing out of NN queries in an untrusted outsourced environment, while at the same time protecting both the POI (Point Of Interest) and querying users' positions. Our techniques rely on mutable order preserving encoding (m-OPE), the only secure order-preserving encryption method known to-date. To reduce the computational cost inherent to processing on encrypted data, and consider the case of incrementally updating datasets in the entire progress.

To Cite This Article: R. Geetha and Dr. K.latha., Skyline Query Endorsement on Unsecure Location. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 80-85, 2015*

INTRODUCTION

The blend of mobile devices and Cloud-based solutions is creating a resourceful ecosystem for reshaping the way geospatial data are stored, managed, served, and shared. In this new ecosystem, also known as database outsourcing, the data owner (DO) delegates the management of its database to a third-party Cloud service provider (SP), and the SP server is responsible for indexing the data, answering client queries, and updating the data on requests from the Dos by using m-OPE.. Probably the most important type of queries that involve location attributes is represented by nearest-neighbor (NN) queries, where a user wants to retrieve the *k* POIs (e.g., restaurants, museums, gas stations) that are nearest to the user's current location (*k*NN).

Performing such queries efficiently, typically using some sort of spatial indexing to reduce the computational overhead. The issue of privacy for users locations has also gained significant attention in past. Note that, in order for the NNs to be determined, users need to send their coordinates to the LBS. However, users may be reluctant to disclose their coordinates if the LBS may collect user location traces and use them for other purposes, such as profiling, unsolicited advertisements, etc. To address the user privacy needs, several protocols have been proposed that withhold, either partially or completely, the users' location information from the LBS. For instance, the work in replaces locations with larger cloaking regions that are meant to prevent disclosure of exact user location. The main idea is to extend existing Private Information Retrieval (PIR) protocols for binary sets to the spatial domain, and to allow the LBS to return the NN to users without learning any information about users locations.

This method serves its purpose well, but it assumes that the actual data points (i.e., the points of interest) are available in plaintext to the LBS. This model is only suitable for general-interest applications such as Google Maps, where the landmarks on the map represent public information, but cannot handle scenarios where the data points must be protected from the LBS itself.

More recently, a new model for data sharing emerged, where various entities generate or collect datasets of POI that cover certain niche areas of interest, such as specific segments of arts, entertainment, travel, etc. For instance, there are social media channels that focus on specific travel habits, e.g., eco-tourism, experimental theater productions or underground music genres. The This category of data owners can benefit greatly from outsourcing their search services to a cloud service provider. In addition, such services could also be offered as plug-in components within social media engines operated by big commerce players. Owing to the specificity of such data, collecting and maintaining such information is an exclusive process,

Corresponding Author: R. Geetha, PG Scholar, Department of CSE, Anna University, BIT Campus, Trichy, India.
E-mail: Geetha15031985@yahoo.co.in

and additionally, some of the data may be perceptive in nature. Some groups may prefer to keep their geo-tagged datasets confidential, and only easy to get to trusted subscribed users, for the fright of backlash from more conservative population groups. It is significant to protect the data from the cloud service provider.

The challenging category of services that provide secure *k*NN processing in out- sourced environments. Specifically, both the POI and the user locations must be protected from the cloud provider.
Our specific hand-outs are:
(i) To propose the VD-*k*NN method for secure NN queries which works by processing encrypted Voronoi diagrams. The method returns exact results, but it is expensive for $k>1$, and may impose a heavy load on the data owner.
(ii) To address the limitations of VD-*k*NN, we introduce T*k*NN, a method that works by processing encrypted Delaunay triangulations, supports any value of *k* and decreases the load at the data owner. T*k*NN provides exact query results for $k=1$, but when $k>1$ the results it returns are only approximate. However, we show that in practice the accuracy is high.
(iii) Outline a mechanism for updating encrypted Voronoi diagrams and Delaunay triangulations that allows us to deal efficiently, in an incremental manner, with changing datasets.
(iv) We propose performance optimizations based on spatial indexing and parallel computation to decrease the computational overhead of the proposed techniques.
(v) Finally,we present an extensive experimental evaluation of the proposed techniques and their optimizations, which shows that the proposed methods scale well for large datasets, and clearly outperform competitors.

Overview of Spatial Query Processing:

A. Data pre-processing:

Initially collecting spatial information and processing those attributes for our relevant development. Process completely maintain by data owner till preserving the entire information. The complete records can be analyzing and only using as final training set. Training the data can be achieve by preprocessing and updated it on correct module. Data-gathering methods are often used to remove the irrelevant & redundant values. Getting the co-ordinates from spatial data & finding the weight contributions of the neighbors.

B. Spatial -NN Progress:

Extracting the relevant information from main dataset will be starting work for this module. Intermediate distance can be calculated by using Euclidean distance form. This calculation can be process by x, y co-ordinates for both restaurants and client side LBS information. Nearest neighbor algorithm used to find object which is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its *k* nearest neighbors.

C. State of art preserving:

Complete information has to keep securely on repository. Data preserving can be processing through cryptographic technique. Updated information has been encrypted by using AES (Advanced Encryption Standard) algorithm. Till the distance evaluation content has been completely encrypted by this 128 bit encryption technique solidly processing each attributes on this encryption process

D. Service outsourcing:

After encryption has been completed, cipher text can be saved in repository. Entire information can be ready to send to third party cloud called outsourcing. As like client-server communication data owner & cloud party will share the encrypted files. At the end cloud not only process for storage side but also work for providing service to client. As per the server socket process, client and server mechanisms can be appeared. Cloud will act as server to receive the content from the owner side provider and owner will act client side work.

E. Spatial provider side conservation:

While receiving from data owners information saving as cipher text. From this type structured format third party could not able to get the original information easily. Spatial details & its neighbors with signatures details storage will avoid the maintenance cost from owner side.

F. User side presentation:

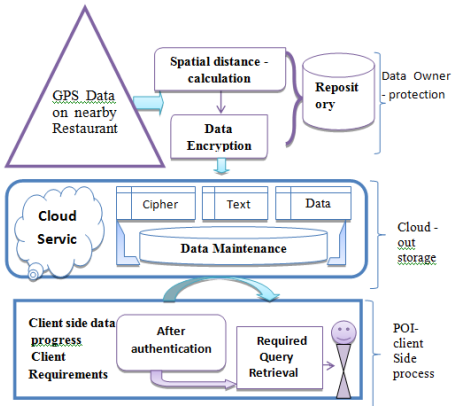
Process can be initializing by Client authentication. This is online progress in between user side & provider side. Points of interest can be retrieving as located in repository when user has been request to the cloud. Final response will include POI with relevant nearby value.

The data owner sends a shadow index to the client. The shadow index is encrypted by the data owner, and the decryption key is given to the server. The client traverses the outline index in order to compute the distance between its query and a node of the index. The client computes encrypted distances and sends them to the server. However, the method requires the entire encrypt index to be transferred to the client. The proposed method from returns a relevant partition $E(G)$ from the entire encrypted dataset, and $E(G)$ is guaranteed to contain the answer for the NN query.

System Model and Assumption:

The system model comprises of three distinct entities: (1) the data owner; (2) the outsourced cloud

service provider (for short cloud server, or simply server); and (3) the client. The data owner has a dataset with *n* two-dimensional points of interest, but does not have the necessary infra- structure to run and maintain a system for processing nearest-neighbor queries from a large number of users. Therefore, the data owner outsources the data storage and querying services to a cloud provider. As the dataset of points of interest is a valuable resource to the data owner, the storage and querying must be done in encrypted form more details will be provided in the privacy model.



The server receives the dataset points of interest from the data owner in encrypted format, together with
some additional encrypted data structures needed for query processing. The server receives *k*NN requests from the clients, processes them and returns the results. while the cloud provider typically possesses powerful computational resources, processing on encrypted data incurs a considerable processing overhead, so performance considerations at the cloud server represent an important concern.

The client has a query point *Q* and desires to find the point's adjoining neighbors. The client sends its encrypted location query to the server, and receives k nearest neighbors as a result. Make a note of that, due to the fact that the data points are encrypted, the client also requests to perform a small part in the query processing itself and an overview of the mutable order preserving encoding (mOPE) use as a build hunk in our work small part in the query dispensation itself.

A. Privacy Model:

The dataset of points of interest represents an important asset for the data owner, and an important source of returns. Therefore, the coordinates of the points should not be known to the server. The server executes correctly the given protocol for processing *k*NN queries, but will also try to infer the location of the data points. It is thus necessary to encrypt all information stored and processed at the server.

To allow query evaluation, a special type of encryption that allows processing on cipher texts is necessary. The use of mOPE technique is a provably secure organizes preserving encryption method, and our techniques inherit the indistinguishability under ordered chosen plaintext attack (IND-OCPA) security guarantee against the truthful but inquisitive server provided by mOPE. Furthermore, there is no collusion between the clients and server, and the clients will not disclose to the server the encryption keys.

B. Secure Query Processing Method:

The processing of kNN queries on encrypted data requires complex operations, but at the core of these operations sits a relatively simple scheme called mutable order-preserving encryption. It allows secure evaluation of range queries, and is the only provably secure order-preserving encoding system (OPES) known to date. The difference between mOPE and previous OPES techniques is that it allows cipher texts to change value over time, hence the mutable attribute. The mOPE operations on plaintext/cipher texts as encoding and decoding, whereas AES (conventional symmetric encryption) operations are denoted as encryption/decryption.

The mOPE scheme in a client-server setting works as follows: the client has the secret key of a symmetric cryptographic scheme, e.g., AES, and wants to store the dataset of cipher texts at the server in increasing order of corresponding plaintexts. The client engages with the server in a protocol that builds a B-tree at the server. The server only sees the AES cipher texts, but is guided by the client in building the tree structure. The algorithm starts with the client storing the first value, which becomes the tree root. Every new value stored at the server is accompanied by an insertion in the B-tree. Figure 2 shows an example where plaintext values are also illustrated for clarity, although they are not known to the server (for simplicity we show a binary tree in the example).

Assume the client wants to store an element with value *55*: it first requests the cipher text of the root node from the server, then decrypts *E(50)* and learns that the new value *55* should be inserted in the tree to the right hand side of the root. Next, the client

requests the right node of the root node and the server sends E *(70)* to the client. The process repeats recursively until a leaf node is reached, and *55* is inserted in the appropriate position in the sorted B-tree, as the left child of node *60*. The client sends the AES ciphertext *E(55)* to the server which stores it in the tree. The *encoding* of value *55* in the tree is given by the path followed from the root to that node, where *0* signifies following the left child, and *1* the right child. In addition, the encoding of every value is padded to the same length (in practice 32 or 64 bits) as follows:

mOPE encoding = [mOPE tree path]10…0

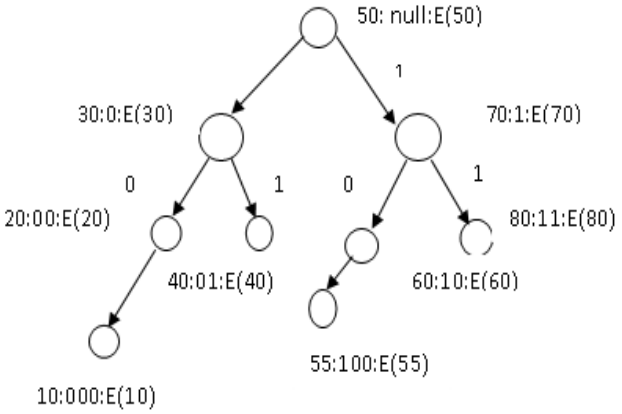


Fig. 2: mOPE Tree: Inserting node *E(55).*

Ciphertext	mOPE Encoding
E(50)	[]1000=8
E(30)	[0]100=4
E(70)	[1]100=12
E(20)	[00]10=2
E(40)	[01]10=6
E(60)	[10]10=10
E(80)	[11]10=14
E(10)	[000]1=1
E(55)	[100]1=9

Fig. 3: mOPE Table.

The server maintains a mOPE table with the mapping from cipher texts to encodings, as illustrated in Figure 3 for a tree with four levels (four-bit encoding). It is an order preserving encoding, and it can be used to answer securely range queries without need to decrypt cipher texts. mOPE satisfies IND-OCPA i.e., indistinguishability under ordered chosen-plaintext attack. The method does not leak anything besides order, which is the intended behavior to support comparison on cipher texts.

C. Incremental Updates:

The locations of datasets are changes quite frequently. Re-generating a new encrypted dataset at the data owner each time some points change incurs a prohibitively expensive overhead. In this context, it is important to address the issue of incremental updates.

For incremental updates, consider only T*k*NN and VD-1NN. In the case of T*k*NN, if a data point moves, the position of the data point is changed and the slopes of *d* edges connected to the data point are also changed. The complexity of the update is $O(d)$,where *d* is the degree of

The data point must be re-encoded with mOPE, whereas the slopes of the edges are re-encrypted with AES encryption. In the preprocessing step, the data owner computes the triangulation and calculates the potential topological events. The data owner builds up a balanced SWAP-tree. In the iteration step, when there is a topological event, the data owner processes the event and updates the SWAP-tree.

The number of pairs of two adjacent triples is equal to the number of edges which is 3*n*. The preprocessing step requires $(nlogn)$ time. The update time is $(logn)$ [14].

There are two separate cases:

(1) The data point *P* moves within the circle. edges including the point *P* and MBR boundaries of the triangles including the point *P* should be updated. The update time is $O(d)$ where *d* is the degree of the data

(2) The data point *P* moves outside the circle. The topology is changed. The time to update the triangulation is $(logn)$.

Experimental Evaluation:

The main recital metrics used to estimate the proposed techniques are query response time and communication cost. The response time measures the duration from the time the query is issued until the results are received at the client. It includes the computation time at the server and the client, as well as the time required for transfer of final and intermediate results between client and server. Communication cost (measured in kilobytes) is important given that many wireless providers charge customers in proportion to the amount of data transferred.

Advantages:

- For the technical reason or maintenance cost data owner save the data into cloud.
- AES is more secure (it is less vulnerable to cryptanalysis than 3DES).
- Cloud violation can be completely avoided by using the proposed technique.
- AES supports larger key sizes than 3DES's 112 or 168 bytes.
- Performance of query processing has been improved on compare with existing technique.
- AES is faster in our required hardware and software specification

Proposed System:

LBS services have been handling by data owner. From the out sourcing process owner has to handling over to cloud party. From the initial work machine learning technique used to train the information which is going to produce. Under the machine learning Data mining uses information from past data to analyze the outcome of a particular problem or situation that may arise. Data mining works to analyze data stored in data warehouses that are used to store that data that is being analyzed. That particular data may come from all parts of business, from the production to the management. Managers also use data mining to decide upon marketing strategies for their product. They can use data to compare and contrast among competitors.

Cloud party using this information and use the client details for unwanted advertisements. From this proposal cloud service provider (i.e. third party) could not able to get the original data. K-Nearest neighbor algorithm is a data mining technique used to get the nearby values in GPS data. To preserve the entire data we are using AES-Advanced encryption standard algorithm to encrypt. Gathering information and performs machine learning technique for training the data. Each step information storage lead to solve the missing identification process. By using this AES algorithm helps us to converting plain values to the cipher test in order to give one by one encryption progress. That is update or modulates on working data at any time.

Conclusion:

The mutable order-preserving encoding (mOPE) as building block. Euclidean distance formulation provides exact results, but its performance overhead may be high. kNN only offers approximate NN results, but with better performance. In addition, the accuracy of kNN is very close to that of the exact method. To investigate more complex secure evaluation functions on cipher texts skyline queries and also research formal security protection guarantees against the client, to prevent it from learning anything other than the received k query results.

Future Work:

In prospect work plan to investigate more complex secure evaluation functions on cipher texts, such as skyline queries. Well also research formal security protection guarantees against the client, to prevent it from learning anything other than the received *k* query results.

REFERENCES

A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, Order Preserving Symmetric Encryption, EuroCrypt'09.

A.Boldyreva, N. Chenette, and A.O'Neill, Order Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions, Crypto'11.

Ali Khoshgozaran and Cyrus Shahabi, Blind Evaluation of Nearest Neighbor Queries Using Space Transfor-mation to Preserve Location Privacy, SSTD'07

Bin Yao, Feifei Li and Xiaokui Xiao, Secure Nearest Neighbor Revisited, ICDE'13.

Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi and Kian-Lee Tan, Private Queries in Location Based Services: Anonymizers are not Necessary, SIG-MOD'08.

Gabriel Ghinita, PanosKalnis, Murat Kantarcioglu, and Elisa Bertino, A Hybrid Technique for Private Location-Based Queries With Database Protection, SSTD'09.

Gabriel Ghinita, PanosKalnis, Murat Kantarcioglu, and Elisa Bertino, Approximate and exact hybrid algorithms for private nearest-neighbor queries with database pro-tection, Geoinformatica'11

Gruteser M. and Grunwald D., Anonymous usage of location-based services through spatial and temporal cloaking, MOBISYS'03.

Haibo Hu, Jianliang Xu, Chushi Ren and Byron Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism, ICDE'11.

Huiqi Xu, Shumin Guo and Keke Chen, Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation, TKDE'12.

Jon Louis Bentley, Multidimensional Binary Search Trees used for Associative Searching, ACM Communications, 1975.

Mark de Berg *et al*., Computational Geometry, Springer.

Raluca Ada Popa, Frank H. Li and Nickolai Zeldovich, An ideal-Security Protocol for Order-Preserving Encod-ing, IEEE S&P'13.

Thomas Roos, Voronoi diagrams over dynamic scenes, Discrete Applied Mathematics, 1993

Wong, W.K., David W. Cheung, Ben Kao and Nikos Mamoulis, Secure kNN Computation on Encrypted Databases, SIGMOD'09.